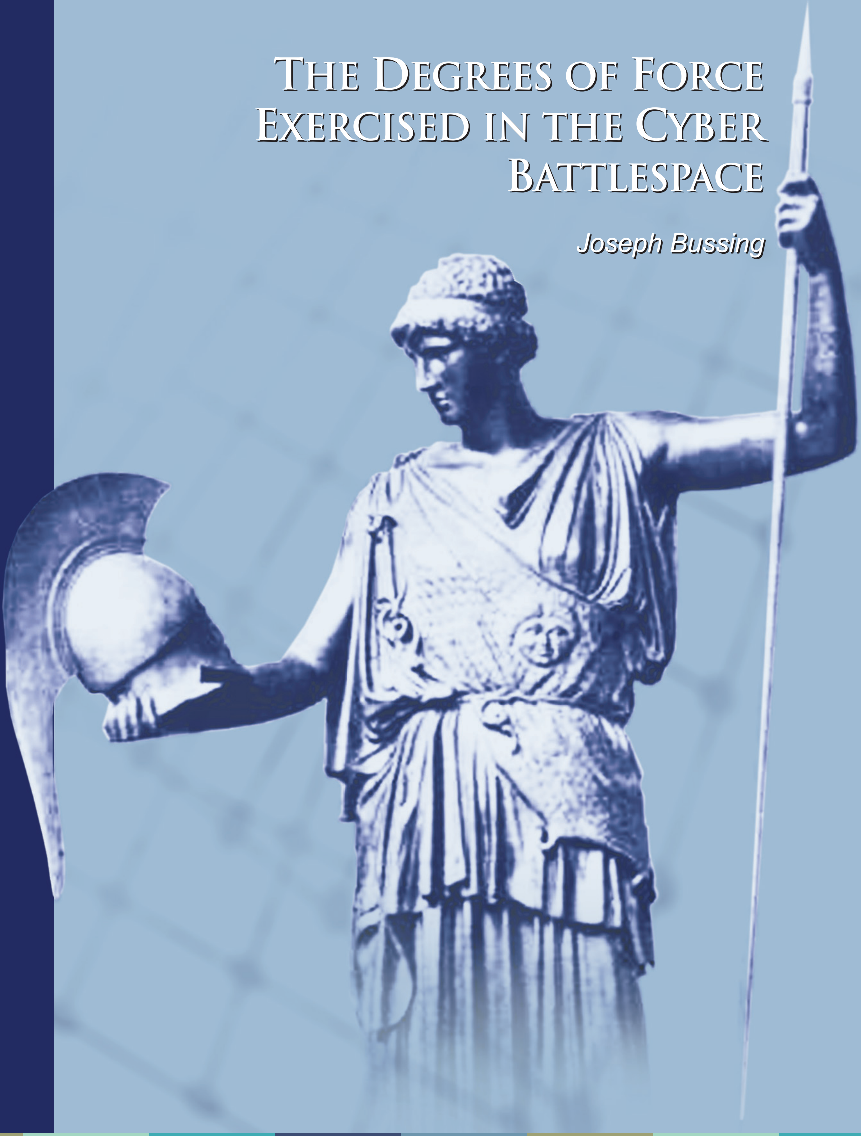
CONNECTIONS

THE QUARTERLY JOURNAL

THE DEGREES OF FORCE EXERCISED IN THE CYBER BATTLESPACE

Joseph Bussing



Common Ground: U.S. and NATO Engagement with Russia in the Cyber Domain
Geoff Van Epps

Security Agencies and Parliamentary Committees of Inquiry in Germany: Transparency vs. Confidentiality
Sebastian von Münchow

Energy Security: A Paradigm Shift
Velichka Milina

The Young and the Normless: Al Qaeda's Ideological Recruitment of Western Extremists
Thérèse Postel

PARTNERSHIP FOR PEACE CONSORTIUM OF DEFENSE ACADEMIES AND SECURITY STUDIES INSTITUTES

FALL 2013

Partnership for Peace Consortium of Defense Academies and Security Studies Institutes

The PfP Consortium Editorial Board

The PfP Consortium Publication Manager

The articles appearing in all *Connections* publications do not necessarily represent the views of the authors' institutions, their governments, or the PfP Consortium itself.

The Consortium's family of publications is available at no cost at http://www.connections-qj.org. If you would like to order printed copies for your library, or if you have questions regarding the Consortium's publications, please contact the PfPC Operations Staff at pfpcpublications@marshallcenter.org.

CONNECTIONS

The Quarterly Journal

Volume XII, Number 4 Fall 2013

The Degrees of Force Exercised in the Cyber Battlespace

Joseph Bussing [*]

Introduction

Each instance of communication via the Internet depends on the transfer of confidential, readily available, and authenticated information. If this information is read, altered, or forged in any way, it jeopardizes the secure and safe operation of any service depending on the transfer of data. Thus, the exploitation of data can be leveraged in ways that can have devastating effects on modern societies. The problem with a networked society is that the international conventions on the use of force fail to sufficiently safeguard the world from the instability caused by computer attacks. This article seeks to remedy the situation by defining what kinds of actions carried out via computerized networks constitute a use of armed force or armed conflict.

This article applies the existing Laws of Armed Conflict (LOAC) to three cases of computer-based attacks carried out by nation-states. In doing so, the aim is to highlight the legal limitations on actions that can be taken to respond to computer attacks. The first examination involves the wave of cyber attacks that precluded the 2008 South Ossetia War between Russia and Georgia. The second case addresses the United States' covert operation, codenamed "Olympic Games." For this case, the analysis will be focused on the Stuxnet computer program. The third case utilizes LOAC to assess the acts of digital espionage carried out by the Chinese People's Liberation Army Unit 61398.

Using LOAC as a legal rubric, the cases suggest that there are three distinct interpretations of computer-based operations. The case of the 2008 South Ossetia War constitutes a situation in which using computers to attack another country can be interpreted as a use of force and as an act of armed conflict. The "Olympic Games" operation reveals that a computer-based attack can be considered a use of force but not an act of armed conflict. The analysis of the actions of Unit 61398 shows a perspective on computer attacks that are neither a use of force nor an act of armed conflict. Each case expresses unique characteristics of operations in cyberspace. Therefore, in order to develop a legal understanding of these cases, the analysis favors an effects-based assessment of cyber attacks, pioneered by Michael Schmitt and expressed in the Tallinn Manual on the International Law Applicable to Cyber Warfare.[1]

[*] Joseph Bussing was born and raised in the Silicon Valley of California. He is a recent graduate of The New School's Graduate Program of International Affairs and a self-taught computer programmer.

[1] Michael N. Schmitt, gen. ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013).

Developing a Legal Framework of Cyber Attacks Through an Effects-Based Approach

Computer-based attacks represent a subset of actions that can be described as information operations. Information operations (IO) are defined as actions taken by the military in times of peace or war to affect adversary information and information systems while defending one's own information and information systems.[2] Broadly speaking, IO refers to radar jamming, psychological, and electronic means of carrying out operations. A subset of electronic IO is called computer network operations (CNO). CNO are defined as operations to attack, deceive, degrade, disrupt, deny, exploit, and defend electronic information and infrastructure.[3] Two sub-elements of CNO are attack and defense. Computer network attacks (CNA) are defined as actions taken via computer networks to disrupt, deny, degrade, or destroy the information within computers and computer networks and/or the computers themselves.[4] If the information within a computer that controls the water level in a nuclear power plant suffers any disruption to the information flow, it can have devastating physical effects.[5] Each case presented in this article represents a form of CNA with its own unique effect. The effects highlighted by each case range from denial of service and theft of information to physical destruction.

Due to the relatively new nature of state-sponsored international cyber attacks, this article addresses the existing body of international treaty law that includes the prohibitions on the use of force and self-defense as found in the United Nations Charter. These will be used to measure the extent to which computer-based attacks can be considered a use of force. Additionally, the effects-based guidelines will be used as a normative framework for determining the level of force for each case in this article.

Article 2(4) of the UN Charter acts to maintain international peace and order by prohibitive means. It prescribes that "all members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations."[6]

Despite the intentions of this statement, the vague terminology "use of force" presents challenges for maintaining the prohibitive elements of Article 2(4). This idea was

[2] Joint Chiefs of Staff, Joint Pub. 3-13, "Information Operations" (13 February 2006), Gl-3; available at http://www.carlisle.army.mil/DIME/documents/jp3_13.pdf.

[3] Ulhas Kirpekar, "Information Operations in Pursuit of Terrorists," Master's Thesis completed at the Naval Postgraduate School, Monterey, CA (September 2007), 63; available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.185.907&rep=rep1&type=pdf. See also Joint Chiefs of Staff, Joint Pub. 3-13, "Information Operations," II-9 for Cyberspace Operations.

[4] Kirpekar, "Information Operations in Pursuit of Terrorists," 63.

[5] World Nuclear Association, "Fukushima Accident 2011" (2013), available at http://www.world-nuclear.org/info/Safety-and-Security/Safety-of-Plants/Fukushima-Accident-2011/#.UXgxAIJAvIU.

[6] United Nations, Article 2, paragraph 4.

introduced at the 1945 San Francisco Conference, when the Brazilian delegation argued that Article 2(4) ought to include economic coercion.[7]

This amendment to Article 2(4) never occurred, and the unclarified concept of force is further expressed in the 1986 International Court of Justice ruling on *Nicaragua v. United States*. The Court considered that the supply of funds to the Nicaraguan *contras*, while an act of intervention in the internal affairs of Nicaragua, did not amount to a use of force.[8] This ruling suggests that the instruments of force ought to be evaluated on the basis of their outcomes. For example, physical coercion has a higher probability of causing destruction, injury, and escalation than diplomatic or economic coercion. Therefore, the effects of armed force are perceived as more concerning, and thus armed action prohibited by the international community. From this concern, force is divided into a spectrum of severity that ranges from armed to economic. Thus, the challenge is to place the diversity of computer attacks on this spectrum of force.

Chapter VII, Article 41 of the UN Charter further defines the spectrum of force by establishing specific acts that are considered to be non-armed uses of force. Non-armed uses of force include "complete or partial interruptions of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communications."[9] Because Article 41 uses the wording "other means of communications," it includes network technology in this level of non-armed force. The conflict of this legitimization of computer-based weapons arises when network technology is manipulated to cause physically destructive events.

Chapter VII, Articles 39 and 51 of the UN Charter authorize the use of force based on specific criteria established for the preservation of peace and self-defense. Article 39 grants the UN Security Council the "authority to determine the existence of any threat to peace, breach of peace, or act of aggression."[10] Article 51 authorizes the use of force with the expression that "nothing in the present Charter shall impair the inherent right of individual and collective self-defense if an armed attack occurs against a Member of the United Nations."[11] Under this structure, there is no use of the term "use of force." Instead, "armed attack" gives a state the right to respond in self-defense.[12] As a result, the Security Council is the only entity that may mount forceful responses to events that

[7] Doc. 215, I/1/10, 6 U.N.I.C.O Docs. 559 (1945). See Doc. 784, I/1/27, 6 UNICO Docs. 334-35 (1945). The amendment proposed by Brazil, that would have added to the prohibition on the threat or use of force the words "and from the threat or use of economic measures," was rejected by a 26–2 vote.

[8] Military and Paramilitary Activities (Nicaragua v. U.S.), 1986 I.C.J. 4,119 (27 June 1986). The court did not actually apply Article 2(4); instead, the Court applied the customary international law prohibition on the resort to force to adjudicate the issue.

[9] United Nations Charter, Article 41.

[10] United Nations Charter, Article 39.

[11] United Nations Charter, Article 51.

[12] Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thought on a Normative Framework," *Columbia Journal of International Law* 37:3 (1999): 893.

threaten the peace. States using the Article 51 authorization must define "armed attacks" before using any kind of force. For states responding to computer attacks, the difficulty is in determining whether a computer attack is a threat to peace, a breach of peace, an act of aggression, or something that constitutes an imminent armed attack.

The legal frameworks regarding the prohibition on the use of force and the self-defensive authorization of force are challenged by computer-based attacks because they have a wide range of effects. They vary from annoyance to physical destruction. One category of computer attack that is interpreted as a definite use of force is an attack that directly causes physical damage.[13] The difficulty is in situating computer attacks that do not cause physical damage or injury within the spectrum of force. Given that the international community already recognizes actions at various levels of force (e.g., economic coercion or materially supporting rebels in another state), computer attacks must also be considered in a similar way. Therefore the Schmitt criteria are used to describe the various thresholds of force for a given attack based on the characteristics of their effects.

The following characteristics are used to asses the extent to which non-physically destructive computer attacks amount to a use of force: severity, immediacy, directness, invasiveness, measurability, and presumptive legitimacy.[14]

- Severity measures whether or not an attack is physically destructive or merely diplomatic coercion. This quality considers the Article 2(4) definition that takes into account the territorial integrity or political independence of a state.
- Immediacy measures how fast an attack occurs. For armed attacks, the effects are immediate, as in the example of an exploding bomb. Even though computer attacks travel at the speed of light, they may take time for their effects to be known.
- Directness is a measure of how connected the attack is to the effect of the attack. In the case of traditional armed attacks, the missile causes the destruction. In cases of economic coercion, like currency manipulation, the effects of this attack are less certain.[15]
- Invasiveness measures the degree to which attacks occur inside or outside a country. In traditional armed attacks or uses of force, attacks occur within a country's territory.
- Measurability is similar to directness, except it is a measure of how easy it is to measure the effect of an action.
- Finally, presumed legitimacy takes into account the legal norms and considerations that authorized the attack.

[13] Ibid., 898.

[14] Ibid., 898–99.

[15] Daniel Ikenson, *Appreciate This: Chinese Currency Rise Will Have a Negligible Effect on the Trade Deficit* (Washington, D.C.: CATO Institute, 2010), available at www.cato.org/publications/free-trade-bulletin/appreciate-chinese-currency-rise-will-have-negligible-effect-trade-deficit.

This framework is useful because it provides a thorough set of guidelines for analyzing all types of force and attacks, including computer-based forms. The six criteria are especially helpful in describing the degree with which a computer attack may be considered a non-armed use of force or an armed use of force.

As an additional concept of this framework, in cases of computer attacks that are considered to be below the threshold of force as well as armed attack, the right to respond in self-defense is based on the following three factors:

- The attack is part of an overall operation culminating in an armed attack
- The attack is an irrevocable step in an imminent and unavoidable attack
- The defender is reacting in advance of the attack during the last possible window of opportunity.[16]

This second scheme will be applied to the cases of the 2008 South Ossetia War and the actions of Unit 61398 because these cases did not cause physical destruction. Because of the destruction caused by the "Olympic Games" operation, it will be assessed using the effects-based criteria and under the restrictions of U.S. and international law for its authorization to act. Furthermore, the Iranian response to this CNA suggests that when computers cause physical destruction they may be considered as a use of force below the threshold of armed conflict.

The 2008 South Ossetia War Between Russia and Georgia

The biggest problem with computer network attacks, especially those that are part of covert operations waged by nation-states, is attribution. Even if communications can be traced back to a specific computer, it may be impossible to demonstrate a link between that computer and a state to which responsibility can be attributed.[17] For this reason, the case analysis for the 2008 South Ossetia War assumes that branches within the Russian government sponsored the computer attacks that targeted Georgian infrastructure. The difficulty in attribution creates a problem where the legality of cyber attacks can only be discussed *post facto*. This results in a condition where there can be no real-time assessment of the cyber battlespace.

For this case, the assumption that the cyber attacks originated in Russia is made for a number reasons. The first reason is that the focus of this article is on state-sponsored computer attack. While Russia has not claimed responsibility for the computer attacks, if attribution could be made, this case would be a clear example of classifying CNA as an armed conflict and a use of force. The second reason is because when a computer network attack is used to cause unrest in a target country, it is unlikely that the perpetrator will publicly acknowledge or leave traces that can credibly determine their guilt.[18] The

[16] Schmitt, "Computer Network Attack and the Use of Force in International Law," 908.

[17] Daniel Silver, "Computer Network Attack as a Use of Force under Article 2(4)," *International Law Studies* 76, special issue on "Computer Network Attack and International Law" (2002): 79.

[18] Ibid.

third reason is that when computers are used in the context of traditional military operations, states would have little motive to raise a legal dispute solely on the basis of computer-based attacks.[19] This is because a military attack is far more egregious that a computer attack. Finally, it is likely that when states conduct computer attacks they would attempt to conceal their involvement, or to make their efforts look like those of a non-state sponsored hacker.[20]

Despite the lack of attribution in this case, evidence that Russia has been developing its offensive cyber capabilities has been growing. In March 1998, U.S. officials found a connection between intrusions into computers systems belonging to the Pentagon, NASA, the U.S. Department of Energy, private universities, and research labs. All of the attacks had come from a computer network in Russia.[21] Once more, attribution in this battlespace remains uncertain, and the identity of the culprit is still unknown to the public. Another event, this one in 2007, involved a three-week-long, politically charged cyber attack against Estonian computers. The computers reported to have originated the attacks had Russian Internet addresses and were housed at state institutions.[22] The Russian government denied its involvement with these attacks as well. In light of all these events, in 1995 Russian General Vladimir Slipchenko stated that the Russian General Staff Academy had shifted its focus from force-on-force simulation to system-on-system simulations, which included cyber and other information-related systems.[23]

In August 2008, hostilities between Russia and Georgia over the breakaway territory of South Ossetia reached a point of military engagement. On 8 August, Russian tanks crossed the border into Georgia. However, on 7 August computer operations had already been conducted against the computer systems of Georgia.[24] The targets of the cyber attack were Georgian government websites and even included websites of the U.S. and British Embassies. The attacks initially came from Russian IP addresses.[25] Even though this incident was not directly attributable to Russian government agents or military forces, it resulted in a cyber blockade that perfectly correlated with the Russian military to make its offensive more successful.[26] For these reasons, this cyber attack is consid-

[19] Ibid.

[20] Ibid.

[21] "Cyber War; The Warnings?" *PBS Frontline* (2003); available at www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/.

[22] Timothy Thomas, "Nation-State Cyber Strategies: Examples From China and Russia," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry Wentz (Washington, D.C.: National Defense University Press, 2009), 475–76.

[23] Ibid., 476.

[24] Eneken Tikk, et al., "Cyber Attacks Against Georgia: Legal Lessons Identified," report published by the Cooperative Cyber Defense Center of Excellence, Tallinn, Estonia (November 2008), 4; available at http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf.

[25] Jeffrey Carr, "The Rise of the Non-State Hacker," in *Inside Cyber Warfare: Mapping the Cyber Underworld* (Sebastopol, CA: O'Reilly Media, 2009), 15–17.

[26] Richard A. Clarke and Robert K. Knake, "Why Cyber Warfare is Important," in *Cyber Warfare: The Next Threat to National Security and What to Do About It* (New York: HarperCollins, 2010), 18–21.

ered an act of armed conflict, because it was an operational element that prepared the battlespace for a Russian military invasion of Georgia.

The effects of the cyber operation had little to offer in the terms of severity. No one was killed as a direct result of the operation, and no property damage occurred. The CNA against Georgia during the South Ossetia conflict is best characterized as a digital blockade of information. To understand this in the context of international law, the UNGA 3314 on the Definition of Aggression states that a blockade of ports or coastlines is considered an act of aggression.[27] In this case, no physical goods were prevented from entering the country. The digital blockade severed the information pipeline and repopulated it with Russian propaganda, during a time when information confidentiality, integrity, and availability were major priorities.

During this computer attack, websites containing important information were defaced, and Internet communications were jammed by using a flooding technique. The result rendered inoperable the websites of the Georgian president, parliament, government, and foreign ministry.[28] The lack of access to legitimate information coming from the government of Georgia limited the vital dissemination of information flowing between government ministries and the public. An additional element of this attack was that it motivated the National Bank of Georgia to stop offering electronic services for a period of ten days.[29]

The immediacy of the cyber attacks in context of Russia's military incursion into Georgian territory further bolsters the interpretation that this attack represents a use of armed force. Even though the only severe effect of the CNA was communications disruption, it happened at a time when communication was vital to the Georgian government.[30] It also happens that the attacks only lasted for several days, beginning on 7 August 2008.[31] This short duration, which coincided exactly with the Russian incursion into South Ossetia, indicates a directness that connects the harm caused by the cyber attack with the harm inflicted by Russian military forces. On any other day the digital blockade would have been a nuisance, but the temporal proximity to actual military fighting conveys that this was a digital act of armed conflict. Another way of viewing this is to consider the attack as a part of a military operation in the same way that radar jamming or communications disruption serve to contribute to the overall effectiveness of an operation.

The measurability and invasiveness of this operation are limited to cyberspace. Because the method of the attack was to disrupt service and deface websites, the only digital "invasion" that occurred existed within the computers that hosted the following URLs: www.president.gov.ge (the Georgian president's website); www.nbg.gov.ge (the National Bank of the Republic of Georgia); and www.mfa.gov.ge (the Ministry of For-

[27] Definition of Aggression, United Nations General Assembly Res. 29/3314, Annex, U.N. Doc. A/RES/29/3314/Annex (14 December 1974).

[28] Thomas, "Nation-State Cyber Strategies."

[29] "Cyber War; The Warnings?"

[30] Ibid.

[31] Ibid.

eign Affairs of the Republic of Georgia).[32] The denial of service attacks are measured in the flow of information to specific websites. As a standard measurement, the average Mb/s for attacks that were defended by Kaspersky Labs prevention software in 2011 was 70 Mb/s.[33] In a report from a computer security firm that monitors Internet traffic, the attacks against these Georgian websites reached an average of 211.66 Mb/s, and peaked at 814.33 Mb/s, which averaged a length of two hours and fifteen minutes, but reached a peak attack duration of six hours.[34] The measured intensity of the attack on Georgia relative to the average intensity of a similar style attack conveys an extremely organized and calculated effort. Concluding, the measurability and invasiveness of the cyber attack against Georgia further supports the idea that the attack was made in concert with the Russian military, and thus constitutes a use of force and qualifies as an armed conflict.

The presumptive legitimacy of this attack is directly related to the threshold of force established in the United Nations Charter. The current reading of Article 41 suggests that the disruption of digital communications is internationally accepted as being a non-armed use of force. This presumptive legitimate framework suggests that, because this computer attack did not cause physical damage, it is not an act of armed force, but rather an act of non-armed force.

For the reasons stated above, the Schmitt criteria offer a better way of understanding non-armed uses of force in the context of computer attacks. The actions whereby the Russian government distanced itself from the nationalistic hacker community granted the Kremlin the benefit of having plausible deniability while gaining the additional benefit of passively supporting and enjoying the strategic rewards of the hackers' actions.[35] Even though this act is a non-armed use of force under Article 41, the immediacy, directness, invasiveness, and measurability suggest that this attack is an act of armed conflict.

To conclude, if the 2008 South Ossetia cyber attacks did in fact originate from the Russian government, they would be considered an act of armed conflict. The attacks were calculated to have an invasive aspect that directly served as an information blockade immediately before a military invasion. Because of those characteristics, the attack certainly violates the Article 2(4) prohibition on the use of force and qualifies as an act of armed conflict subject to an Article 51 response of self-defense.

Stuxnet – The Cyber Equivalent to Precision-Guided Missiles

The best kind of covert operation is the one that no one ever knows about. The U.S. National Security Act of 1947 defines covert action as an activity or activities of the United

[32] Ibid.

[33] Yury Namestnikov, "DDos Attack in Q2 of 2011," *Securelist* (29 August 2011); available at www.securelist.com/en/analysis/204792189/DDoS_attacks_in_Q2_2011.

[34] Jose Nizario, "Georgia DDoS Attacks—A Quick Summary of Observations," Arbor Networks (12 August 2008); available at http://asert.arbornetworks.com/2008/08/georgia-ddos-attacks-a-quick-summary-of-observations/

[35] Thomas, "Nation-State Cyber Strategies."

States government designed to influence political, economic, or military conditions abroad, where it is intended that the role of the United States government will not be apparent or acknowledged publicly.[36] This definition is in direct conflict with the prohibition on the use of force described in Article 2(4) of the UN Charter. To influence political, economic, or military conditions in another country is to violate that country's political sovereignty, and thereby constitutes an act of force. Whether or not the force is armed or non-armed is subject to debate. Thus, the highest goal of physically destructive covert operations is to remain undiscovered, or plausibly deny involvement.

As was made evident in the ICJ ruling on the *Nicaragua v. United States* case, even if covert operations are discovered, they can function at a level below the threshold of armed conflict. This suggests that, despite the lack of clarity around the terms "armed" or "attack," states agree that not all military actions equate to an armed conflict.[37] Military attacks that clearly violate a state's political sovereignty yet do not constitute armed conflict is a category that can also be said to include the Stuxnet computer attack. For that reason, it is an excellent case to use for analyzing covert computer attacks waged against nation-states, because it is the only example where attribution is absolutely certain and where the cyber attack constitutes a clear use of force.

The "Olympic Games" operation began in 2006 during the second term of the George W. Bush Administration, and lasted until November 2010, during President Obama's first term in office (even though the computer code had a self-deletion date of 24 June 2012).[38] The earliest phases of Stuxnet's development involved lawyers auditing the program code to make sure that the cyber weapon did not violate the laws of armed conflict.[39] Furthermore, the intent of the computer program was not only to hinder the nuclear ambitions of Iran; it was also designed to interfere with Iran's best scientific and military minds.[40] The Stuxnet designers made it seem like sloppy engineering or faulty mechanical hardware were at fault for causing problems. This unresolved issue caused a great deal of stress and instability among the staff working at Natanz.[41] The Stuxnet program had different forms that had affected different systems within the enrichment facility and had caused varying effects. The developers of Stuxnet were constantly changing the modalities of the attack to create new versions of the bug.[42] The end result was a physically destructive and psychologically destabilizing computer attack directed at the country of Iran.

The effects-based analytical guidelines suggest that there are two ways of categorizing this attack. The views can either support or deny the interpretation of this event as an armed attack. The severity of the physical damage caused by the attack is limited to the

[36] SEC. 503 [50 U.S.C. §413b] (para e).

[37] United Nations Charter, Article 39.

[38] David Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York: Crown Publishers, 2012), 202.

[39] Ibid., 193.

[40] Ibid., 199.

[41] Ibid.

[42] Ibid.

tangible destruction of uranium centrifuges located within the Natanz uranium enrichment facility. Thus, according to one interpretation, this computer attack was an act of armed force prohibited by Article 2(4).

The Stuxnet worm was found on computers throughout the Middle East, and in countries as far afield as Indonesia and the United States. Even though the systems of these countries were disrupted, no physical damage resulted. This means that the designers of the attack had made every effort to keep the destructive elements of the worm inside Iran. The designers gave the program an autonomous logic that only triggered the destructive payload upon successful identification of the right computer inside the right network.

Given that this program was active for a duration of four years suggests a level of commitment on par with armed conflicts. In deciding whether or not this use of force constitutes an armed conflict, the criterion of immediacy suggests that this event is indeed an armed attack, because it lasted from the end of the second Bush Administration and went into the beginning of the Obama Administration. Even though the immediacy factor suggests that Stuxnet was an armed conflict, the other elements of the Stuxnet program suggest otherwise.

The kinetic effects of Stuxnet attack are in no ways similar to those caused by missiles or bombs. The attack had a direct effect, which caused the uranium centrifuges in Iran's nuclear facility to malfunction. Despite the physical destruction caused by the worm, it took place in a manner that did not cause harm to humans. The centrifuges were revved up and down during certain times of the month, which damaged them in a way that made it seem as though the Iranians had purchased faulty equipment or had assembled the devices incorrectly.[43] In this way, the cyber weapon's payload employed humane means below the threshold of traditional kinetic armed attacks.

The Stuxnet operation can be measured in two ways: the spread of its accidental outbreak and the physical destruction it caused. A Symantec security report that analyzed Stuxnet listed that 67,000 of the 100,000 worldwide computers infected with the virus were geographically located within Iran.[44] This fact further supports the notion that this was a calculated and targeted use of force. Additionally, this program destroyed one thousand centrifuges at Natanz (11 percent of the total number at the time) and caused a chaotic environment, which strained the engineering staff and likely significantly slowed Iran's ability to enrich uranium from 2006 to 2010.[45]

The biggest question is whether or not this attack had been legitimately authorized, and what was the legal basis of that authorization. Because Stuxnet was such a clear use of force, the following element of the analysis focuses on the presumed legitimacy of the U.S. legal structures that authorized the action. Due to the fact that this was a covert op-

[43] Ibid., 199.

[44] Nicolas Falliere, Liam O'Murchu, and Eric Chien, "W32.Stuxnet Dossier," Symantec Security Response (February 2011); available at www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

[45] Lukas Milevski, "Stuxnet and Strategy: A Special Operation in Cyberspace?" *Joint Force Quarterly* 63 (2011): 69.

eration, it was subject to the rules and regulations governing such actions. Title V of the National Security Act of 1947 describes the various procedures for ensuring accountability of intelligence activities. The President of the United States is the only entity able to authorize covert actions, and is only permitted to do so if the action is necessary to support identifiable foreign policy objectives of the United States and is important to the national security of the United States.[46] Additionally, every determination of the president shall be established in a published finding that meets the following criteria: a written document must be produced within forty-eight hours of the decision to use covert action; a finding may not authorize a covert action that has already occurred; each finding specifies the department, agency, or entity of the United States authorized to participate; each finding shall specify whether any third party to the United States government is authorized to act; and, finally, a finding may not authorize any action that would violate the Constitution of the United States.[47]

In the case of Stuxnet, proposals for covert action against the uranium enrichment facility in Iran came from the U.S. Strategic Command and the National Security Agency. President Bush felt that the cyber attack was a better option for dealing with Iran's nuclear ambitions than traditional military or diplomatic engagements.[48] When Barack Obama became president, he wanted the intelligence community to take control of the operation, and in doing so reviewed and renewed the set of findings related to Stuxnet so that it would allow the United States to influence the politics, economics, or military standing of another country during peacetime.[49] Therefore, using the existing legal guidelines for covert operations, the Stuxnet attack was presumed to be legitimate and compliant with the laws of armed conflict.

The Stuxnet element of the covert operation codenamed "Olympic Games" has been considered an exemplary use of a computer network attack that falls below the threshold of armed attack. This conclusion is extraordinary, because the Stuxnet worm caused physical damage to a nuclear enrichment facility inside the territory of another sovereign country, and no response or reprisal was ever issued. In November 2010, the President of Iran made a statement that the Bushehr nuclear power plant was delayed in becoming fully operational because of technical reasons. Stuxnet and Natanz were never mentioned.[50] In order to understand the groundbreaking nature of this case, replace the computer-based attack with a precision-guided missile. The difference between the means and effects are huge. The difference between these two uses of force is that if a missile were used, it would have caused an international crisis, because missiles damage more than just uranium enrichment centrifuges. The effect of the computer attack was twofold. It hindered the uranium enrichment program at the Natanz facility in Iran, and it ushered in a new way of exercising force through cyberspace.

[46] SEC. 503 [50 U.S.C. §413b] (para a).

[47] SEC. 503 [50 U.S.C. §413b] (para a), 1–5

[48] SEC. 503 [50 U.S.C. §413b] (para e), 191.

[49] SEC. 503 [50 U.S.C. §413b] (para e).

[50] Gary D. Brown, "Why Iran Didn't Admit Stuxnet Was an Attack," *Joint Force Quarterly* 63 (2011): 70.

Unresolved Issues – Chinese Espionage against U.S. Business

There is a method of cyber attack that is currently below the level of force prohibited by Article 2(4), and that falls well below the threshold of armed conflict. The method is known as espionage. The case used to assess the instance of digital espionage is the known existence of the Chinese People's Liberation Army's Unit 61398. The case suggests that there is no legal deterrent or prohibition in place that adequately addresses digital espionage. The laws of armed conflict do not apply to this situation, because the act of digital espionage is considered to be on the same footing as traditional espionage. In some ways, it poses the same concerns as computer crimes carried out by non-state actors.

Despite the limitations of the law of armed conflict, the effects-based criteria outlined above shed light on the scope and scale of damage caused by cyber espionage. According to a report from Mandiant, an independent computer security company, Unit 61398 has stolen information from 150 companies for a period of seven years, and has accumulated more than a hundred terabytes of data.[51] If twenty terabytes of data were printed out on paper, it would fill a line of large moving trucks fifty miles long.[52] This phenomenon has been monitored for a long stretch of time, and has been directly associated with the People's Liberation Army (PLA). This practice represents a large-scale theft of the intellectual capital of U.S. businesses and undermines their competitiveness. Thus, severity can only be judged on the type of information stolen and the effect this has on the profitability of a business.

All of the factors of the effects-based criteria suggest that this is an armed attack, except for the factor severity. By using the classification levels for national security information, Executive Order 12958 provides guidelines whereby the United States can measure the significance of stolen information:

- A Type 1 attack causes a nuisance or inconvenience to the defense or economic security of the United States.
- A Type 2 attack causes damage to the defense or economic security of the U.S.
- A Type 3 attack causes serious damage to the defense or economic security of the U.S.
- A Type 4 attack causes exceptionally grave damage to the defense or economic security of the U.S.

[51] Mandiant APT 1, "Exposing One of China's Cyber Espionage Units" (2013); available at http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

[52] Joel Brenner, *Calm Before the Storm*, Foreign Policy (2011), *available* at www.foreignpolicy.com/articles/2011/09/06/the_calm_before_the_storm.

- A Type 5 attack causes critical damage to the defense or economic security of the U.S.[53]

Thus, the degree to which an espionage attack is determined to be an armed attack depends on the classification of the information stolen.

The dilemma goes back to the problem of *post facto* judgment. First, an attribution must be made, and then the level of force must be determined. In the case of information theft, evaluating the potential significance of terabytes of stolen data can be a long and daunting task, and in most cases the theft would not rise to the level of an armed attack. If these attacks are not prohibited by Article 2(4), and are not evaluated under the law of armed conflict, there is nothing to prevent countries from engaging in this kind of action. The precedent established in the Unit 61398 cases suggests that digital espionage is beyond legal regulation because it is neither a use of force nor an act or armed conflict.

Conclusion

In all applications of the law of armed conflict, three questions are always asked: Is this an armed conflict? What kind of conflict is this? And finally, what type of combatant is involved? This article sought to answer the first question. However, this only addresses the *jus ad bellum* of computer network operations. Furthermore, each incident of computer attack that goes without legal or political repercussions establishes a precedent under which this form of international behavior is acceptable.

There are numerous unresolved issues in this new battlespace, including the legal structure governing the *jus in bello* of computer attacks. The principles of necessity, distinction, and proportionality with regard to autonomously spreading computer programs are collectively a large area of concern. Who are the combatants of a computer attack – the computers, the software, or the programmers, and what rights are these entities afforded? One of the main ways computer code propagates itself is by using treacherous deceit, which violates laws prohibiting perfidy. Because cyberspace is made up of computers that are owned by companies based in other countries, are these companies accountable because they are materially supporting the attack? Furthermore, are cyber conflicts most appropriately considered as international conflicts or domestic conflicts? The questions remain unresolved, and as societies around the globe become more reliant on information and the technological infrastructures that supply it, the conventional understanding of war and international legal structures will need to evolve in order to address the issues and concerns raised by state-sponsored computer-based attacks.

[53] Mark B. Treadwell, "When Does an Act of Information Warfare Become an Act of War? Ambiguity in Perception," U.S. Army War College Strategy Research Project (1998), 16–17; available at www.dtic.mil/cgi-bin/GetTRDoc?AD=ada345572.

Common Ground: U.S. and NATO Engagement with Russia in the Cyber Domain

Geoff Van Epps *

Introduction

Significant changes in the global strategic landscape over the past two decades include the fall of the Iron Curtain and the dissolution of the Soviet Union, accelerated globalization, increasing reliance on digital information technologies in all aspects of life, the rise of China and India, global financial crises, the political revolutions of the Arab Spring, and the emergence of violent Islamist extremism as a key feature of the geopolitical landscape. Yet at the same time, many of the key dynamics of the international arena remain unchanged from twenty years ago, including the volatility and instability of the Middle East, the lack of development in most of Africa, the ever-increasing integration of the global economy, and the preeminence of the United States as an actor in global affairs, with other states, such as the United Kingdom, Germany, and Russia also playing key roles.

Among all that has changed and all that remains the same, new issues have emerged, few of which merit consideration in isolation. Rather, the complex and interconnected nature of today's international system demands analysis that accounts for the relationships between actors and issues and considers the multiplicity of effects that their interaction unavoidably creates. Two key features of the current strategic environment—the two that are the focus of this article—are the indispensability of information technology in all aspects of modern life and the continued significance of Russia as an actor on the global stage.

Driven by the growing dependence of modern society on digital technology and the vulnerability of digital systems to cyber threats, cybersecurity has emerged as a critical national security issue, spawning a growth industry that researches solutions to the technical, legal, and policy challenges of the day. At the same time, the United States and its allies in the North Atlantic Treaty Organization (NATO) contend with a Russian Federation that no longer poses the existential threat of the Soviet superpower era but still wields enough power to demand attention and to play the role of spoiler on many important global issues. The U.S. and NATO have repeatedly and publicly declared improved relations and increased cooperation with Russia to be top priorities, but that rhetoric has seldom translated to concrete improvement in their relationships or broad advancement across the agenda of critical topics. However, cybersecurity is an area of strategic importance where real progress is possible. The June 2013 announcement of a new U.S.–Russia bilateral agreement to work together on cybersecurity is an important

* Geoff Van Epps is a lieutenant colonel in the US Army. This article is based on research he conducted while serving as a Senior Fellow at the George C. Marshall European Center for Security Studies in Garmisch, Germany, from 2012-2013.

symbolic first step in that direction, but the accord is modest, and should merely serve as a starting point for a longer-term and more extensive program of cooperation. More tangible improvement of U.S. and NATO relations with Russia is vital, given the interconnectedness of all three actors and their status as the three most important actors in modern European—and to some extent global—security affairs. Given Russia's robust cyber capability (and demonstrated willingness to employ it), its longstanding quest for recognition as a leader in world affairs, and the public call to develop international norms for cyberspace, cybersecurity is a prime topic for U.S. and NATO engagement with Russia.

Complex Interdependence and Cyberspace

United States engagement with Russia is inevitable as both countries rank among the few states with both global interests and the ability to advance those interests. NATO, too, is inextricably bound to the U.S., with whom it shares many common values and objectives, while its geographic proximity to Russia and its intertwined (and occasionally competing) security interests make constant interaction with the Russian Federation unavoidable and highly important.

The growing entanglement between the U.S. and NATO, on one side, and Russia on the other is therefore not surprising. As globalization has accelerated and technology has advanced over the past quarter-century, the expenses associated with transportation and communication have plummeted, greatly reducing the effects of distance on economic, military, social, and other aspects of interaction between states, organizations, and even individuals.[1] Declining costs have generated a rise in the volume of interactions between these actors, conveying additional costs and benefits to all parties involved and creating a situation where each player in the web of relationships maintains a degree of interdependence on the others.[2] This interdependence—defined as the mutual dependence between parties or the ability of those parties to reciprocally affect one another—is the hallmark of globalization and the defining feature of the modern international system.[3]

The idea that actors in the international system interrelate in ways that make them reliant on one another, that this reliance extends across nearly all dimensions of their relationships, and that the behavior of those actors is affected as a consequence is both simple and powerful. The theory gained credibility and widespread acceptance over the past three decades, moving it rapidly into the mainstream of international political thought and influencing the development of foreign policy for the United States and many other countries, particularly the advanced industrial and post-industrial democracies. Applying the notion of complex interdependence to world affairs has had a recur-

[1] Joseph S. Nye, *Understanding International Conflicts*, 4th ed. (New York: Longman, 2003), 185–92.

[2] Robert O. Keohane and Joseph S. Nye, *Power and Interdependence*, 3rd ed. (New York: Longman, 2001), 7–9.

[3] Joseph S. Nye, "Independence and Interdependence" (1976), in Nye, *Power in the Global Information Age* (New York: Routledge, 2004), 154; Keohane and Nye, *Power and Interdependence*, 7.

sive effect on the international system, simultaneously shaping how international actors view their relationships, craft their policies, and choose to behave while also offering plausible explanations for how and why those behaviors cause events to unfold on the world stage as they do. At the same time, an idealistic view of interdependence has fed the expectation that interdependence—especially complex interdependence, with its deepened relationships along multiple dimensions—would lead to an inexorable decline in international conflict by increasing constraints on belligerent behavior, building a sense of community among global actors, and reducing incentives for conflict.[4] Yet while complex interdependence has grown in importance and acceptance, it has not fulfilled hopes for increased global peace and cooperation.[5] Largely, this is because interdependent relationships deepen and strengthen ties between actors, but such interdependencies still can result in competition and even conflict. Most significantly, even in non-zero sum situations, where all parties benefit from a relationship, asymmetries exist, and the distribution of gains is uneven among the actors involved. As a result, interdependence does not mean uniform cooperation and an end to conflict. Rather, it creates conditions that simultaneously encourage greater cooperation in some areas while fostering conflict in others.[6]

Cyberspace provides a clear illustration of an arena where actors engage in both collaboration and fierce competition, often among the same actors and frequently at the same time. The rapid development and spread of advanced information technologies over the past few decades has generated a cyber dimension to complex interdependence that has its own unique characteristics. This information revolution has powered radical changes in politics, business, culture, and other aspects of society, spawning new types of community, encouraging the growth of organizations as networks, creating demands for new roles for government, and generally challenging hierarchical bureaucracies while fostering a trend toward decentralization.[7] The consequences of this shift are hard to overstate. Bureaucracies, whether corporate or governmental, are undercut by formal and informal organizations that more rapidly and efficiently share and process information to influence larger groups of people more quickly than traditional institutions. Individuals and private organizations have joined states as direct players in world politics. As this has occurred, the façade of the inviolable and immutable sovereignty of states has showed signs of change, with transnational communications granting the masses the

[4] The tradition of belief that interdependence will mark the end of war can be traced to before World War I in works such as Norman Angell, *The Great Illusion: A Study of the Relation of Military Power in Nations to Their Economic and Social Advantage* (New York: Putnam, 1910). A post-Cold War analysis of the effect of interdependence on interstate conflict is Susan M. McMillan, "Interdependence and Conflict," *Mershon International Studies Review* 41 (1997): 35–36.

[5] Nye, *Understanding International Conflicts*, 195.

[6] Nye, "Independence and Interdependence," 154.

[7] Nye, "The Information Revolution and American Soft Power" (2001), in Nye, *Power in the Global Information Age* (New York: Routledge, 2004), 81–82.

ability to engage on issues that were formerly the sole preserve of governments.[8] Such changes have not been uniform across the globe—their emergence has been much faster in the "zone of democratic peace," while virtually nonexistent in underdeveloped regions—but they nonetheless represent an order of magnitude shift in the contact among societies and demonstrate the potential for even broader alteration of the status quo.[9]

At the same time that they have instigated such drastic societal change, many of these developments have served only to reinforce the characteristics of complex interdependence: the emergence of powerful non-state global actors; the importance of non-security issues like the economy and the environment; and the effects on the ease of use of military force in an age of mass media, whistleblowers, and social networking. The computer networks that enable many of these changes—cyberspace—allow international actors to "embrace" one another by digital connection with speed, ease, and frequency.[10] Indeed, the essence of cyberspace is its connectivity, and as the volume of international digital transactions continues to grow for the foreseeable future, the ties that bind connected actors in the international system will strengthen further, and their interdependence will increase.[11] At the same time, cyberspace's unique nature, its relative immaturity as a medium, and the lack of widely accepted norms for operating within it will pose new challenges that will affect these relationships and potentially change the dynamics of complex interdependence in new and unpredictable ways.

Cyberspace and Cybersecurity

Digital interconnectedness has become a ubiquitous feature of modern life, both a cause and an effect of the growing interdependence that defines the international system. Information technology penetrates and enables every facet of society. Explosive growth in the connection of computers and computer-enabled equipment over networks that permit the rapid communication of vast amounts of information at steadily declining costs has driven changes so profound that the development and diffusion of these technologies is widely seen as comparable in scope and impact to the Industrial Revolution.[12] Digital technology now underpins the function of our world, providing the means to communicate globally, buy and sell goods and services, execute financial transactions, manage air traffic, track and predict weather, operate critical infrastructure, control industrial systems, direct the operations of military units, and perform thousands of other vital functions with unprecedented speed and precision. These developments have conveyed tremendous benefits globally, but they have not come without accompanying challenges.

[8] Ibid., 83–88.

[9] Keohane and Nye, *Power and Interdependence*, 217–18.

[10] Will Goodman, "Cyber Deterrence: Tougher in Theory than in Practice?" *Strategic Studies Quarterly* 4:3 (Fall 2010): 102-35, quote on p. 121.

[11] International Telecommunications Union, *Measuring the Information Society 2012* (Geneva: International Telecommunications Union, 2012) is the annual report by the UN specialized agency that attempts to quantify the breadth and depth of the spread of information and communications technology globally.

[12] Nye, *Understanding International Conflicts,* 215,

The most prominent of these concerns is cybersecurity, which encompasses a set of related technical, policy, and legal issues that could collectively threaten the positive-sum outcomes achieved by the current webs of global interdependence and thereby alter the basis of many current, key relationships in the international system.[13]

Collectively, the information technology networks—and the hardware, software, connective lines, and data that constitute them—that facilitate our digital interconnectedness have become known as cyberspace, a complex and ever-changing manmade environment that is partly physical and partly virtual.[14] Its unique nature makes merely conceptualizing cyberspace a challenge, and achieving consensus on the exact definition of cyberspace has been elusive.[15] Most definitions, however, are consistent with the U.S. military's description of cyberspace as a "global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[16] However, the lack of agreement on what cyberspace *is* remains problematic because it affects how actors view the medium and subsequently develop capabilities, craft policies, and ultimately decide to act on cyber issues.[17]

Difficulty defining cyberspace leads inevitably to key conceptual debates whose eventual resolution will strongly influence subsequent thinking about cyber topics. As an important example, embedded in the U.S. military's definition is the idea of cyberspace as the fifth domain for military operations (along with land, sea, air, and space), which has policy and doctrine implications that can complicate discussions with allies, adversaries, and even other U.S. government stakeholders in discussions of cybersecurity issues. The U.S. Department of Defense made the conceptual leap to define cyberspace as an operational domain as "an organizing concept for DOD's national security missions" in order to "take full advantage of cyberspace's potential."[18] This declaration does not resolve the theoretical debate within DoD entirely; on the contrary, it merely provides a common conceptual framework for discussing cyber-related issues and serves more as a new starting point for discussion than a definitive end point for thinking about cyber-

[13] James C. Mulvenon and Gregory J. Rattray, "Addressing Cyber Instability: Executive Summary," *Cyber Conflict Studies Association Web Site* (9 July 2012), 1; available at www.thecre.com/fnews/wp-content/uploads/2012/07/CCSA-Addressing-Cyber-Instability.pdf.

[14] Nye, *Cyber Power* (Cambridge, MA: Belfer Center for Science and International Affairs, 2010), 4.

[15] Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz (Washington, D.C.: National Defense University Press, 2009), 24. A summary of definitions of U.S., U.K., Canadian, and Australian terms can be found in David J. Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power* (New York: Routledge, 2011), 36.

[16] United States Department of Defense, *Dictionary of Military and Associated Terms,* Joint Publication 1-02 (Washington, D.C.: Government Printing Office, 2011), 77.

[17] Betz and Stevens, *Cyberspace and the State*, 36-37.

[18] United States Department of Defense, *Strategy for Operating in Cyberspace* (Washington, DC: Government Printing Office, 2011), 5.

space.[19] At the same time, theory or policy developed from this point of view is less valuable when trying to harmonize actions with other actors who do not view cyberspace in the same terms.

Perhaps the best model for visualizing the networks of information systems themselves is offered by RAND scientist Martin Libicki, who describes cyberspace as consisting of three layers. The first layer, which undergirds the other two, is the physical components consisting of "boxes and (sometimes) wires" that forms the hardware of the information system. The middle layer is syntactic, containing the software with instructions and protocols that allow the hardware devices to function and communicate with one another. The uppermost layer is the semantic layer, containing the system's information – and therefore the reason the system exists.[20] Libicki's model helps structure discussions of cyberspace by adding shape, scope, and tangibility to the concept, but like all models it has limitations and may not withstand the test of time as the complexity of information systems continues to grow and new technologies change the design and function of these systems.

Another important ongoing debate deals with whether or not cyberspace constitutes an international commons. Those who argue that cyberspace is a commons do so because it shares characteristics with the other global commons of air, sea, and space, and because the idea of a global commons is widely understood and accepted. The most significant contribution of the idea of cyberspace as a commons is that, by definition, the global commons do not fall under the jurisdiction of a single country and their joint use is governed by international norms – much as many authorities argue is the case with cyberspace today.[21] Those experts who reject the idea of cyberspace as a commons find fault with the idea that the Internet is borderless and that nation-states have no ability to exercise sovereignty within cyberspace. In their view, nearly all of the infrastructure comprising cyberspace—the physical layer, to use Libicki's construct—resides within the borders of a sovereign state and is, therefore, subject to the laws of that state.[22] Re-

[19] Franklin D. Kramer, "Cyberpower and National Security: Policy Recommendations for a Strategic Framework," in *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz (Washington, D.C.: National Defense University Press, 2009), 12. See also Rattray, "An Environmental Approach to Understanding Cyberpower," in *Cyberpower and National Security,* for a more extensive analysis.

[20] Martin Libicki, *Cyberdeterrence and Cyberwarfare* (Santa Monica, CA: RAND, 2009), 12–13.

[21] Leon E. Panetta, "America's Pacific Rebalance," *Project Syndicate* (31 December 2012); available at http://www.project-syndicate.org/commentary/renewing-the-us-commitment-to-the-asia-pacific-region-by-leon-e--panetta. See also James C. Stavridis and Elton C. Parker, III, "Sailing the Cyber Sea," *Joint Forces Quarterly* 65 (2012): 62; and Mark Barrett, Dick Bedford, Elizabeth Skinner, and Eva Vergles, *Assured Access to the Global Commons* (Norfolk, VA: Supreme Allied Command Transformation, North Atlantic Treaty Organization, 2011), xii–xiii.

[22] James Lewis, "Rethinking Cyber Security—A Comprehensive Approach," speech to the Sasakawa Peace Foundation, Tokyo, Japan (12 September 2011); available at http://csis.org/files/publication/110920_Japan_speech_2011.pdf. See also Nye, *Cyber Power*, 15.

solving this debate will affect the further development of cyberspace, its architecture, governance and the values that shape it.[23] Meanwhile, disagreement on this fundamental notion impedes progress toward international consensus on rules for operating in cyberspace and on who bears responsibility for enforcing those norms.

Deficient Security

However one conceives of cyberspace, the rapid spread of and increased reliance on information technology has in many cases outstripped the ability of governments to regulate its use or even to understand the problems new technologies create. The debates on how to define cyberspace, whether or not to think of it as an operational domain, and whether or not it constitutes a global commons are important but abstract. On the other hand, the fact that most of the infrastructure of what has evolved into modern-day cyberspace is built with technology that was developed with no consideration of a need for security features is a concrete problem that has made securing cyberspace an almost Sisyphean task. The original designers of the Internet were researchers at four universities in the western United States who used federal government funding in the 1960s to create a network allowing computers at their schools to communicate directly with one another. The connection was designed in a decentralized manner in order to promote scalability, privacy, and ease of communication rather than security. Its inventors envisioned linking thousands of well-intentioned academics and scientists to exchange research – not the billions of machines and users executing the vital and occasionally sinister functions of today.[24]

As the Internet matured, grew in size, and spread from academia to government to broad civilian use, the underlying fact that the technological building blocks of the Internet were designed without security in mind emerged as its core technical problem. Today, in the words of one expert, "connectivity is currently well ahead of security."[25] Openness and ease of use have inevitably attracted malicious actors, whose sophistication and ambition grew along with the Internet, evolving from mild web page defacement in the 1990s to highly organized cyber crime syndicates and state-directed espionage and cyber attack programs today.[26] The U.S. recognizes this vulnerability, with President Barack Obama describing in a 2009 speech "the great irony of our Information Age – the very technologies that empower us to create and to build also empower those who would disrupt and destroy."[27] Consequently, early in his presidency, the Obama Administration completed a Cyberspace Policy Review and expanded the Comprehen-

[23] Lewis, "Rethinking Cyber Security."

[24] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Harper Collins, 2010), 81-83.

[25] Kenneth Geers, *Strategic Cyber Security* (Tallinn, Estonia: Cooperative Cyber Defence Center of Excellence, 2011), 10.

[26] Mulvenon and Rattray, "Addressing Cyber Instability," 1–2.

[27] Barack Obama, "Remarks by the President on Securing our Nation's Cyber Infrastructure," 29 May 2009; available at www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

sive National Cybersecurity Initiative to confront "one of the most serious economic and national security challenges we face as a nation."[28]

U.S. partners and allies also acknowledge the gravity of cyber threats and are working to address the issue. In its 2010 *Strategic Concept*, NATO's description of the security environment noted, "Cyber attacks are becoming more frequent, more organised and more costly in the damage that they inflict on government administrations, businesses, economies and potentially also transportation and supply networks and other critical infrastructure; they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability."[29]

Similarly, Russia and China have also expressed concern about the threat posed by inadequate cybersecurity, most publicly in a letter they submitted, along with the governments of Tajikistan and Uzbekistan, to the United Nations General Assembly in 2011, calling for an international code of conduct for information security. Their proposal described the "need to prevent the potential use of information and communication technologies for purposes that are inconsistent with the objectives of maintaining international stability and security."[30] This theme is also echoed in Russia's 2013 Foreign Policy Concept, which calls for an international code of conduct for information security under UN auspices and commits to countering actions with "purposes that run counter to international law, including actions aimed at interference in the internal affairs and constituting a threat to international peace, security, and stability."[31]

All Threats Are Not Created Equal

Recognizing the fundamental lack of security in cyberspace is a necessary first step toward addressing the problem, but it is not sufficient to achieve a solution. The vulnerability opens a window to several threats, each of which targets different portions of cyberspace, has different objectives, poses a different risk to national security, and requires different solutions to mitigate. As with other cybersecurity issues, no clear consensus on classifying these threats has emerged. The U.S. Department of Defense, focused primarily on defending U.S. government computer networks, recognizes two principal categories of threat: computer network attack (CNA) and computer network exploitation

[28] Office of the President of the United States, *Comprehensive National Cybersecurity Initiative* (Washington, D.C.: The White House, 2009), 1; available at http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf.

[29] North Atlantic Treaty Organization, *Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization* (Brussels: NATO, 20 November 2010), 11; available at www.nato.int/nato_static/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf.

[30] "Letter Dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations Addressed to the Secretary-General," Sixty-sixth Session of the United Nations General Assembly, 14 September 2011.

[31] Ministry of Foreign Affairs of the Russian Federation, "Concept of the Foreign Policy of the Russian Federation," 12 February 2013; available at http://www.mid.ru/brp_4.nsf/0/76389FEC168189ED44257B2E0039B16D.

(CNE).[32] Political scientist Joseph Nye, in a broader and more useful view of the hazards in cyberspace, sees four activities that threaten national security: espionage, crime, war, and terrorism.[33]

War and terrorism are potentially the most immediately destructive threats in cyberspace, and they correlate closely to the U.S. DoD category of computer network attack. The recently constituted U.S. Cyber Command (USCYBERCOM) is the DoD organization working to defend against these threats along with protecting defense networks against espionage. However, the USCYBERCOM mandate only extends to defending some portions of the U.S. government network; it has no responsibility for most of the civilian federal government systems, state or local government networks, or any of the private-sector digital infrastructure or the transportation, energy, finance, or communications systems they control.[34] The U.S. Department of Homeland Security bears the burden of securing the non-defense portion of the federal government network, but there is no federal agency responsible for securing the country's most critical privately-owned infrastructure from cyber attack.[35] For the NATO Alliance as a whole, responsibility is similarly fragmented, with member states taking ownership of the security of their own networks and NATO assuming responsibility from the point where NATO and national networks connect inward to shared Alliance networks.[36]

Espionage and crime may pose less immediately destructive threats than cyber war or terror attacks, but they are the most costly security threats the U.S. currently faces.[37] Cyber crime has become a highly organized and phenomenally profitable illicit activity, where modern international business practices merge with cutting-edge technology to

[32] Jayson M. Spade, *China's Cyber Power and America's National Security* (Carlisle, PA: U.S. Army War College, 2012), 7.

[33] Nye, *Cyber Power*, 16.

[34] Richard A. Clarke, "War from Cyberspace," *The National Interest* (November/December 2009): 33–34.

[35] Ibid., 34–35. A recent executive order expanded programs to share information on cyber threats between the federal government and the private sector, established voluntary cybersecurity best practices for critical infrastructure providers, and called for incentives to encourage compliance with the standards. See Office of the President of the United States, "Executive Order – Improving Critical Infrastructure Cybersecurity," 12 February 2013; available at www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity. However, with the U.S. Congress unwilling or unable to pass laws like the Cybersecurity Intelligence Sharing and Protection Act (CISPA) or the Cyber Security Act of 2012 to legislate information sharing programs and technical security standards, many of the most obvious and significant vulnerabilities in the U.S. remain unaddressed.

[36] North Atlantic Treaty Organization, "Defending the Networks: The NATO Policy on Cyber Defence," 4 October 2011; available at http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf.

[37] Nye, *Cyber Power*, 16.

outpace corporate and law enforcement attempts to combat the threat.[38] Internet security firm McAfee estimated in a widely quoted report that cybercriminals stole a staggering USD 1 trillion in data and intellectual property in 2008.[39] A competing firm, Symantec, issued its own annual report for 2012 and calculated more narrowly and conservatively that consumer cybercrime accounted for USD 110 billion in losses.[40] The lack of agreement on what constitutes a cybercrime combined with uneven reporting protocols makes pinpointing the exact scope of the problem difficult, but the rough order of magnitude is clear – and it is huge.[41] Notwithstanding its scope, cybercrime is, for most countries, including the U.S., not viewed as a direct threat to national security, and therefore is not an issue that the defense establishment addresses. Largely left to the law enforcement community, international cooperation to deal with cybercrime is uneven, in spite of the first international convention on cybercrime having been signed a dozen years ago. Troublingly, many of the countries where cybercrime activity is highest, most notably Russia, have not accepted international norms on cybercrime and lack either the ability or the will to curb the online criminal activity occurring within their borders.

Cyber espionage, on the other hand, is closely related to cyber crime, and has the full attention of defense ministries around the world. However, the distinction between commercial espionage, which is often considered a form of cybercrime, and defense-related espionage is not always apparent. Cyber espionage, taken as a whole, is a significant threat, but dealing with it is problematic because, at the most basic level, espionage is widely practiced and not illegal under international law.[42] Nations have conducted espionage since ancient times, and there are few incentives for them to curb activities that provide intelligence that contributes to national security and international stability.

[38] Clay Wilson, “Cyber Crime,” in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz (Washington, D.C.: National Defense University Press, 2009), 415.

[39] McAfee and SAIC, *Underground Economies: Intellectual Capital and Sensitive Corporate Data Now the Latest Cybercrime Currency* (28 March 2011), 5; available at www.ndia.org/Divisions/Divisions/Cyber/Documents/rp-underground-economies.pdf. This estimate has proven controversial in cybersecurity circles, because the number is shockingly large and because the figure has subsequently been repeated in speeches by President Obama, General Alexander from CYBERCOM, and members of Congress. Analysis of the USD 1 trillion loss estimate can be found, among other sources, at Misha Glenny, “Why You Can’t Trust the Cybercrime Stats,” *Wired UK* (6 November 2011); available at www.wired.co.uk/magazine/archive/2011/12/ideas-bank/cybercrime-stats. See also Andy Greenberg, “McAfee Explains the Dubious Math behind Its ‘Unscientific’ $1 Trillion Data Loss Claim,” *Forbes* (3 August 2012); available at www.forbes.com/sites/andygreenberg/2012/08/03/mcafee-explains-the-dubious-math-behind-its-unscientific-1-trillion-data-loss-claim; and Peter Maass and Megha Rajagopalan, “Does Cybercrime Really Cost $1 Trillion?” *Pro Publica* (1 August 2012); available at www.propublica.org/article/does-cybercrime-really-cost-1-trillion.

[40] Symantec, *2012 Norton Cybercrime Report* (5 September 2012), 3; available at www.norton.com/ 2012cybercrimereport.

[41] Wilson, “Cyber Crime,” 428–29.

[42] James Lewis, “Five Myths about Chinese Hackers,” *Washington Post* (22 March 2013).

However, cyber espionage has some unique features that distinguish it from traditional espionage. Because it is "in many ways easier, cheaper, more successful and has few consequences,"[43] more countries are likely to participate in cyber espionage and do so more often.[44] Even now, losses to espionage annually are enormous. More important than the financial loss, however, is the transfer of invaluable intellectual property to potential adversaries, especially technologically advanced potential peer competitors like China and Russia. The head of U.S. Cyber Command, General Keith Alexander, labeled the losses "the greatest transfer of wealth in history" in a 2012 speech at the American Enterprise Institute,[45] and former White House official Richard Clarke wrote of his concern that they "might swing the balance of power in the world away from America."[46]

Just as the distinction between cyber espionage and cyber crime is a slight one, the differences between espionage and attack in the cyber realm are equally subtle.[47] In fact, intrusion into a network to commit an attack appears virtually identical to an act of espionage in the initial phases,[48] and code left behind by intruders to enable further spying could be virtually indistinguishable from a program planted to damage the system in a later attack.[49] Every act of trying to gain access to a system without authorization—whether erroneously, out of curiosity, or for malicious purposes—is almost indistinguishable to the system administrators charged with defending a network, and large numbers of attempts make it difficult to identify the serious threats from all the white noise of ongoing network activity. In a 2010 speech, General Alexander claimed that "DOD systems are probed by unauthorized users approximately 250,000 times an hour, over 6 million times a day."[50] While each probe does not necessarily constitute an attack, let alone a serious one, the sheer volume of potentially harmful activity demands attention and has driven the search for solutions.

As a final complication, simply recognizing—and classifying— a threat in cyberspace is challenging, but identifying the source of the threat is often an even greater problem. Attribution of any activity in cyberspace is incredibly difficult. Every actor in cyberspace can hide behind a veil of anonymity because of weak standards for creden-

[43] Clarke and Knake, *Cyber War*, 232.

[44] Ibid., 228–37.

[45] Gen. Keith Alexander, "Cybersecurity and American Power," Keynote Address to the American Enterprise Institute, 9 July 2012; available at http://www.aei.org/events/2012/07/09/cybersecurity-and-american-power/.

[46] Clarke and Knake, *Cyber War*, 237; Greg Masters, "Global Cybercrime Treaty Rejected at U.N.," *SCMagazine* (23 April 2010); available at www.scmagazine.com/global-cybercrime-treaty-rejected-at-un/article/168630/.

[47] Andrew Cutts, "Warfare and the Continuum of Cyber Risks: A Policy Perspective," in *The Virtual Battlefield: Perspectives on Cyber Warfare*, ed. Christian Czosseck and Kenneth Geers (Amsterdam: IOS Press, 2009), 69.

[48] Libicki, *Cyberdeterrence and Cyberwarfare,* 16.

[49] Libicki, *Cyberdeterrence and Cyberwarfare,* 24–25; Clarke, "War from Cyberspace," 33–34.

[50] Gen. Keith Alexander, "U.S. Cybersecurity Policy and the Role of U.S. CYBERCOM," CSIS Cybersecurity Policy Debate Series (3 June 2010), 6; available at http://csis.org/files/attachments/100603csis-alexander.pdf.

tialing and verifying user identity, and this anonymity is reinforced by the technical ease of masking an actor's identity, location, or the routing of his online activities.[51] In practical terms, this renders malicious actors in cyberspace virtually immune from discovery, as current digital forensic techniques are often inadequate for providing irrefutable proof of their identities. It also makes determining state responsibility for activities in cyberspace a laborious undertaking, as governments claim plausible deniability for actions that appear to emanate from their territory but cannot be proven to do so.[52]

No Simple Solutions

In spite of the seriousness of the vulnerabilities in cyberspace, finding solutions is not simple. The problems resemble webs of Gordian knots, often requiring cross-disciplinary approaches that combine complicated solutions with technical, legal, and policy components and often have unintended consequences in the *terra incognita* of cyberspace.[53] The complexity, overlap between problem areas, and difficulty in coordinating and standardizing responsibility for addressing issues has resulted in slow progress both nationally and at the international level.

Perhaps the most significant challenge has been the lack of an international legal regime or of any emergence of broadly accepted norms for cyberspace, either as an expanded application of existing rules or through the creation of new frameworks specific to the issue.[54] This gap is a function of the lack of a clear body of law that immediately translates to the new challenges arising in cyberspace, coupled with cyberspace's growing importance outrunning the glacial pace of developing international legal standards.[55] Without such a framework, discussion between nation-states about what constitutes acceptable behavior remains more theoretical than practical, and the consequent list of unsolved problems is eye-opening. For example, issues of state responsibility for malicious acts in cyberspace emanating from or passing through a country's borders remain an un-

[51] Geers, *Strategic Cyber Security*, 95.

[52] Determining state responsibility for a cyber incident has two components: degree of involvement and degree of certainty. Each of those dimensions exists along a scale from low to high, meaning that an outside observer can determine varying extents of state involvement in the activity behind the incident, and can do so with different levels of certainty. The more certain of the state's role and the higher the state's level of involvement, the greater responsibility that state bears for the incident.

[53] Maeve Dion, "Different Legal Constructs for State Responsibility," in *International Cyber Security Legal & Policy Proceedings 2010*, ed. Eneken Tikk and Anna-Maria Talihärm (Tallinn, Estonia: Cooperative Cyber Defence Center of Excellence, 2010), 69.

[54] The *Tallinn Manual* is a peer-reviewed but unofficial attempt to remedy this serious deficiency by an international group of experts to interpret existing international law in a cyber context. Less than a year old, the eventual influence of this document has yet to be determined. See Michael N. Schmitt, gen. ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013).

[55] Rex Hughes, "A Treaty for Cyberspace," *International Affairs* 86:2 (2010): 533.

resolved and contentious issue.[56] Cybercrime remains essentially unchecked, and responsibility for responding to cross-border criminal activities is not automatically assigned or consistently acknowledged. The absence of a universal definition of beyond-the-pale behavior that constitutes a legitimate *casus belli* between states leaves unclear the lines that, if crossed, could lead to international conflict. And without a regime to provide consequences for bad behavior, it is nearly impossible to prevent disruptive or provocative actions that could forestall the emergence of standards of conduct or even serve as an outright threat to peace.[57]

Furthermore, the national frameworks for dealing with cyber-related issues, from crime to espionage to military doctrine, are often incomplete, out of date, or inadequate. Some national legal codes fail to provide even the most basic tools for combating digital fraud and theft, let alone more sophisticated or emerging criminal threats. Even the most advanced national strategies and frameworks have gaps or create tradeoffs, seeking different ways to balance, for example, responsibility for cybersecurity between government and the private sector, or the relative importance of security compared to civil liberties.[58] These national policies, in turn, are poorly harmonized internationally, even among close partners, due to the lack of global norms and differing national priorities.

Differences in prioritizing the agenda for international cybersecurity stem from fundamentally divergent understandings of the nature of cyberspace and acceptable behavior in the cyber domain. Some states, like China and Russia, consider existing international law inadequate, advocate a new international treaty to deal specifically with operations in cyberspace, value sovereignty over international cooperation, and view Internet content as a potential threat to their political stability that demands tight controls. On the other side of the debate, most advanced democracies share a view that international law can be effectively applied to cyber issues, consider a new cyber law treaty unnecessary, welcome international cooperation even at the expense of some sovereignty, and view access to the Internet and the free flow of information as fundamental rights. These incompatible perspectives complicate the development of international law on cyber issues and pose an obstacle in nearly all discussions on these matters, as the key players struggle to find common ground for cooperation on even the most fundamental issues.[59]

[56] Goodman, “Cyber Deterrence,” 112–13.

[57] Lewis, “Rethinking Cyber Security.”

[58] A repository of national cyber strategies and policies is on the NATO Cooperative Cyber Defence Centre of Excellence web page at http://ccdcoe.org/328.html.

[59] Carr, *Inside Cyber Warfare* (Sebastopol, CA: O’Reilly Media, 2010), 34–35. For a representative example, see Masters, “Global Cybercrime Treaty Rejected at U.N.” The East-West Institute and Moscow State University’s Information Security Institute have partnered in a Track 2 effort to develop consensus terminology for cybersecurity. Their first round of work produced agreement on twenty basic terms in April 2011; see Karl Frederick Rauscher and Valery Yashchenko, “Russia-US Bilateral on Cyber Security: Critical Terminology Foundations,” April 2011; available at www.ewi.info/system/files/reports/Russia-U%20S%20%20 bilateral%20on%20terminology%20v76%20%282%29.pdf. A follow-on program is underway to expand the agreed-upon lexicon even further.

As a consequence of the lack of international norms and the inconsistency of national frameworks for addressing cyber issues, "bad actors" in cyberspace—whether states, groups, or individuals—often operate beyond the reach of the victims who seek to retaliate or obtain redress for the harm that has been done to them. Shortcomings of this nature create gaps that may be exploited and lead to friction between parties. In some cases, security breaks down to the point that conflict erupts.

When Security Fails

In spite of the relative newness of cyberspace, the wide range of newsworthy cybersecurity incidents is eye-catching. The full spectrum of potential threats to national security in cyberspace may not yet be apparent, but a brief survey of the major incidents demonstrates both the evolving seriousness and variety of threats with national security implications, many of which are historically unique and have established new precedents or pose new challenges for the international community.

Early and comparatively low-impact cybersecurity incidents extend back in time to the Cold War, when the United States reportedly corrupted a Soviet spying operation by allowing oil pipeline control system components to be stolen with malicious programming that resulted in the pipeline's eventual and spectacular malfunction, producing a tremendous explosion that was the largest non-nuclear explosion ever recorded.[60] During the Second Intifada in the Palestinian Territory in 2000, Israeli government hackers disabled the public web pages of the Palestinian National Authority and Hezbollah in an attempt to disrupt command and control of the uprising. Palestinian operatives responded with cyber attacks against Israeli banks and government computer systems, sparking a sort of "cyber holy war."[61] Israel also used offensive cyber techniques to fool Syrian air defense radar as part of the Israeli Air Force bombing of a suspected Syrian nuclear site in September 2007.[62]

A long-running, shadowy espionage operation known as Titan Rain occurred from roughly 2003 to 2005, involving the systematic infiltration of U.S. and Western European government computer networks.[63] Widely judged to be a Chinese government program, the spying effort netted ten to twenty terabytes of data from U.S. military networks alone.[64] Attempts to block penetrations while they were ongoing were often futile, and the stealthy nature of the intrusions made even identifying when the networks were

[60] Clarke and Knake, *Cyber War*, 92–93. Other sources dispute that report, like, for example, Jeffrey Carr, "The Myth of the CIA and the Trans-Siberian Pipeline Explosion," *Digital Dao* (7 June 2012); available at http://jeffreycarr.blogspot.com/2012/06/myth-of-cia-and-trans-siberian-pipeline.html.

[61] Kenneth Geers, "Cyberspace and the Changing Nature of Warfare," *SC Magazine* (27 August 2008); available at www.scmagazine.com/cyberspace-and-the-changing-nature-of-warfare/article/115929/.

[62] Clarke and Knake, *Cyber War*, 1–11.

[63] Brian M. Mazanec, "The Art of (Cyber) War," *Journal of International Security Affairs* (Spring 2009); available at www.securityaffairs.org/issues/2009/16/mazanec.php.

[64] Carr, *Inside Cyber Warfare*, 4.

compromised, for how long, and what data was stolen a matter of educated guesswork.[65] Titan Rain appears to be part of broader, long-term Chinese cyber espionage efforts sometimes referred to as an Advanced Persistent Threat (APT), and subsequent similar operations attributed to China include hacking of computer systems belonging to members of the U.S. Congress and a massive exfiltration of highly sensitive designs for U.S. defense contractor Lockheed Martin's cutting-edge F-35 Joint Strike Fighter program.[66] Although Titan Rain and related espionage programs are almost certainly of Chinese origin, China's steadfast denials are neither surprising nor unusual given the difficulty of ironclad attribution in cyberspace. Likewise, the vulnerability of even the most sensitive data to theft or corruption and the high payoff of cyber espionage programs at relatively low risk make operations of this kind increasingly likely to occur without the civilizing influence of the implicit rules of the road that have evolved to govern traditional spying.[67]

The first major interstate cyber conflict began in April 2007 when the Estonian government moved a Soviet-era Second World War memorial from its prominent location in the middle of the capital, Tallinn, to a military cemetery outside the city center. The decision sparked a vociferous reaction from Russia and from the ethnic Russian minority within Estonia, escalating to violent clashes among partisans on both sides of the issue and quickly devolving into riots and looting in the Tallinn city center. The clashes spilled over into cyberspace, where highly-wired Estonia was extremely vulnerable to disruptions of its government, financial, law enforcement, and media web sites during three weeks of increasingly intense and highly coordinated attacks.[68] Although the cyber assaults ultimately caused more inconvenience than actual damage, the incident was seminal in several important ways.[69] It was the first major, broadly aimed cyber attack on a country's government and industry as part of an international conflict and was serious enough to warrant an Estonian request for consultation with its NATO Allies under the provisions of the Atlantic Charter.[70] It also raised important questions about the

[65] Clarke and Knake, *Cyber War*, 124–26.

[66] Spade, *China's Cyber Power*, 5.

[67] Nye, "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* (Winter 2011): 31.

[68] Geers, *Strategic Cyber Security,* 84–86.

[69] Rain Ottis, "Case Studies on Cyber Conflict – Estonia 2007 and Stuxnet 2010," Presentation at the George C. Marshall European Center for Security Studies, Garmisch-Partenkirchen, Germany, 22 October 2012.

[70] Ulf Häußler clarifies that the only formal consultation of a NATO member with the North Atlantic Council (NAC) under the provisions of the North Atlantic Treaty was when Turkey made the request in February 2003, just prior to the resumption of hostilities against Iraq. Although discussions at the NAC did occur in the context of the 2007 Estonia cyber attacks, neither the Council nor Estonia explicitly mentioned Article 4 in conjunction with the talks. See Häußler, "Cyber Security and Defence from the Perspective of Articles 4 and 5 of the NATO Treaty," in *International Cyber Security Legal & Policy Proceedings 2010*, ed. Christian Czosseck and Karlis Podins (Tallinn, Estonia: Cooperative Cyber Defence Center of Excellence, 2010), 104–5.

thresholds for the use of force and armed attacks under international law.[71] Although Russia denied responsibility, and digital forensics were unable to prove conclusively that the Russian government was behind the attacks, the totality of the evidence strongly suggests Russian state encouragement, and perhaps direction, of the attacks.[72] The Russian government's deniability in this case arose from the involvement of "patriotic hackers," who the Russian government claimed were merely incensed, Internet-savvy citizen activists, mobilized and self-organized to execute highly-coordinated attacks against specific Internet targets using tens of thousands of hijacked computers from 177 countries with no state support or assistance.[73] The disavowal of responsibility, now exceedingly common in subsequent cases, underscores the challenges of attribution and state responsibility in cyberspace. It also highlights challenges that would emerge again in later cyber incidents.

During the August 2008 Russia–Georgia War, cyber attacks synchronized with Russian ground and air operations paralyzed the Georgian ".ge" internet domain by flooding the system's servers with an unmanageable torrent of Web traffic. Government, banking, and media Web sites were overwhelmed, and even the national mobile phone network was eventually incapacitated.[74] The most significant effects were the Georgian government's inability to communicate effectively—particularly in telling its side of the story during hostilities with Russia—and the disruption of public services, especially banking, electricity, and telecommunications.[75] As with the Estonian incident, Russia strongly denied state responsibility for the cyber component of the war, although it unquestionably enjoyed strategic benefits brought about by the cyber attacks on Georgia,[76] and the organizers of the attacks clearly had foreknowledge of the ground war and assistance (if not direction) in planning, organizing, reconnoitering, and synchronizing their activities with Russian military actions.[77]

A more narrowly directed cyber operation uncovered in 2010 shed light on a newer and less public form of cyber conflict. A covert U.S.-Israeli operation named Olympic Games targeted the Iranian nuclear program.[78] One of the Olympic Games computer viruses called Stuxnet contained code that searched for specific software and hardware

[71] Scott J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," *Berkeley Journal of International Law* 27 (2009): 196–97.

[72] Kara Flook, "Russia and the Cyber Threat," American Enterprise Institute Critical Threats (13 May 2009); available at www.criticalthreats.org/russia/russia-and-cyber-threat. See also Carr, *Inside Cyber Warfare,* 3; and Goodman, "Cyber Deterrence," 111.

[73] Eneken Tikk, Kadri Kaska, and Liis Vihul, *International Cyber Incidents: Legal Considerations* (Tallinn, Estonia: Cooperative Cyber Defence Center of Excellence, 2010), 18–25.

[74] Clarke and Knake, *Cyber War*, 17–21.

[75] Tikk, Kaska and Vihul, *International Cyber Incidents*, 77–79; Goodman, "Cyber Deterrence," 115.

[76] Carr, *Inside Cyber Warfare*, 15–19.

[77] Flook, "Russia and the Cyber Threat."

[78] David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *The New York Times* (1 June 2012).

configurations unique to Iranian uranium enrichment centrifuge facilities. Once it found the right combinations, it took control of the machinery and forced it to operate outside its normal parameters, interfering with the enrichment process, damaging the equipment, and causing confusion among the scientists and administrators leading the program.[79] Stuxnet was "the first attack of a major nature in which a cyberattack was used to effect physical destruction," according to former CIA director and retired Air Force General Michael V. Hayden. "Somebody crossed the Rubicon."[80] Indeed, Stuxnet was technically innovative and a watershed in terms of causing physical damage, which arguably exceeded the legal threshold for a use of force, if not an armed attack, under international law. However, since the U.S. and Israel have never formally acknowledged their roles, it also raised again the standard problems with attribution and state responsibility and further reinforced the need for concerted collective action to address the continuing challenges of cybersecurity.

Russia's Role

Russia, for all its problems, still plays a highly significant role in the international system. For a variety of reasons, it maintains sufficient power in its post-Soviet incarnation to be decisive on issues of vital importance to the international community. Though its relations with the U.S., Europe and its neighbors in the post-Soviet space are sometimes rocky, the Russian Federation's combination of physical size, geostrategic position, military brawn, economic might, natural resources, and other factors demand that Russia be considered, if not consulted, in addressing nearly every important topic on the international agenda.[81] In many cases, Russia wields sufficient influence to determine when and how key problems are resolved – or whether they will continue to fester. In spite of this critical role, or perhaps because of it, the United States and its NATO Allies struggle to maintain consistently favorable, productive, and cooperative ties with Moscow, and find it virtually impossible to transform their relationships into stable and meaningful partnerships that take advantage of their deep interdependencies and the many issues where their interests overlap.

Winston Churchill famously commented in a 1939 BBC radio address, "I cannot forecast to you the action of Russia. It is a riddle wrapped in a mystery inside an enigma, but perhaps there is a key. That key is the Russian national interest."[82] Churchill's apt observation is no less true today than it was almost three-quarters of a century ago. Russia, like most countries, will act in its own interest – or in the best interests of its national leadership. Nonetheless, understanding Russia's interests and divining how Russia will

[79] Ottis, "Case Studies on Cyber Conflict"; Sanger, "Obama Order."

[80] Sanger, "Obama Order."

[81] Stephen J. Blank, "Introduction," in *Prospects for U.S.-Russian Security Cooperation*, ed. Stephen J. Blank (Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 2009), 1.

[82] Winston Churchill, "The War Memoirs of Winston Churchill," *Life Magazine* (10 May 1948): 63.

behave to further them is no easy matter.[83] The inscrutable Russian psyche affects foreign policy decisions, as Russian leaders seek to restore national prestige and earn anew the respect of the international community by demonstrating strength, assertiveness, and decisiveness in their external relations. Outside of Russia, this approach often translates to perceived arrogance or even aggressiveness in Russian behavior, leading to tempestuous relationships and borderline-erratic patterns of interaction with other countries.[84]

In spite of the lack of apparent existential threats to the Russian Federation, Russian politicians often display an attitude of insecurity against external threats and a view of the international environment as an incubator for potential menaces.[85] This outlook—and its incongruence with the broader world's view of Russia's security situation—explains much of the friction resulting from Russia's foreign policy. Viewed through this lens, Russia's consistent efforts to maintain influence in the "near abroad" of former Soviet republics and to ward off what it views as unhelpful meddling by outside powers such as the U.S., China, and Europe is designed to stabilize its periphery, buffer against outside threats, and permit the country to concentrate on domestic matters.[86] Similarly, NATO's expansion into Eastern Europe and the former Soviet Union has been vigorously opposed by Russia, with discussions of membership for Ukraine and Georgia around NATO's 2008 Bucharest Summit provoking particularly strident objections. While an impartial analysis would view NATO as a model security institution that provides regional stability that benefits the Russian Federation, Russia's opinion of NATO is quite different, seeing the Alliance as a historic rival and potential threat as it encroaches on strategically vital territory on the Russian border and threatens Russia with encirclement.[87] The European Union's Eastern Partnership has likewise been met with Russian skepticism, with Moscow holding the view that the initiative is an attempt to lure several former Soviet republics out of the Russian orbit.[88]

These long-standing difficulties have been accompanied over the years by friction over a rotating agenda of issues, recently including U.S. plans for missile defense, efforts at democracy promotion,[89] public shaming over Russia's poor human rights re-

[83] Samuel A. Greene and Dmitri Trenin, *(Re) Engaging Russia in an Era of Uncertainty*, Policy Brief 86 (Washington, D.C.: Carnegie Endowment for International Peace, December 2009), 4; Andrei Shleifer and Daniel Treisman, "Why Moscow Says No," *Foreign Affairs* (January/February 2011): 122–38.

[84] David J. Kramer, *The Russia Challenge: Prospects for US-Russian Relations*, Policy Brief (Washington, D.C.: The German Marshall Fund, 2009), 2.

[85] Olga Oliker, Keith Crane, Lowell H. Schwartz, and Catherine Yusupov, *Russian Foreign Policy: Sources and Implications* (Santa Monica, CA: RAND Project Air Force, 2009), 2 and 83–84.

[86] R. Craig Nation, *Results of the "Reset" in US-Russian Relations*, Russie.Nei.Visions No. 53 (Paris: IFRI, 2010), 9; Oliker, et al., *Russian Foreign Policy*, 93–95.

[87] Linas Linkevicius, "Reset with Russia, but with Reassurance," *International Herald Tribune* (9 September 2010); Nation, *Results of the "Reset*," 13-14; Shleifer and Treisman, "Why Moscow Says No."

[88] Kramer, *The Russia Challenge*, 4.

[89] Oliker, et al., *Russian Foreign Policy*, xvi.

cord,[90] and disagreement over Libya, Syria, and Iran.[91] Relations with the West reached their nadir during Russia's August 2008 war against Georgia, when Russia's reputation suffered serious damage and Western cooperation with Russia ground to a halt.[92] After several months of deadlock, in February 2009 U.S. Vice President Joseph Biden announced the Obama Administration's desire to "press the reset button" on its relations with Russia, reversing a "dangerous drift" and emphasizing a list of common interests, including nuclear proliferation, international terrorism, and stability in Afghanistan.[93]

The results of the reset have been inconclusive. Some experts view it as having accomplished what was intended by thawing relations between the U.S. and Russia and reigniting cooperation on Afghanistan, sanctions against Iran, Russian entry into the WTO, and a new strategic arms reduction treaty.[94] Other observers are less sanguine, pointing to a slow erosion of the reset's initial promise through disagreement over Iran and Syria, questions over the legitimacy of Putin's 2012 presidential election victory, passage in the U.S. of the Magnitsky Act to sanction Russian officials who violate human rights, Russian war games simulating an invasion of Poland, and other aggravations.[95] The ultimate value of the reset may never be clear, but the need for the U.S. and NATO to continue a policy of engagement with Russia remains unchanged.

With relationships that are increasingly interdependent and interests that converge on many issues, the U.S. and NATO clearly recognize that cooperation with Russia is a necessity, and that the absence of cooperation comes at a cost.[96] Following a bilateral meeting with then-President of the Russian Federation Dmitry Medvedev in 2012, U.S. President Barack Obama affirmed this view, saying that "as two of the world's leading powers, it's absolutely critical that we communicate effectively and coordinate effectively in responding to a wide range of situations that threaten world peace and security…. [A]t a time of great challenges around the world, cooperation between the United

[90] Commission on U.S. Policy toward Russia, *The Right Direction for U.S. Policy toward Russia* (Washington, D.C.: The Nixon Center, March 2009), 13–14; Dmitri Trenin, et al., *The Russian Awakening* (Moscow: Carnegie Moscow Center, 2012), 8.

[91] Nation, *Results of the "Reset,"* 23; David M. Herszenhorn and Nick Cumming-Bruce, "Putin Defends Stand on Syria and Chastises U.S. on Libya Outcome," *The New York Times* (21 December 2012).

[92] Robert Coalson, "Former U.S. State Dep't Official Pifer Asks, 'Are the Russians Ready to Reengage?'" *Radio Free Europe/Radio Liberty* (19 November 2012).

[93] Craig Whitlock, "'Reset' Sought on Relations with Russia, Biden Says," *Washington Post* (8 February 2009).

[94] Stephen Sestanovich, interview by Bernard Gwertzman, "Reassessing the U.S.-Russia 'Reset'," Council on Foreign Relations Web Site (13 December 2012); available at www.cfr.org/russian-federation/reassessing-us-russia-reset/p29659.

[95] Anne Gearan, "Sour U.S.-Russia Relations Threaten Obama's Foreign Policy Agenda," *Washington Post* (14 January 2013); Thomas E. Graham and Dmitri Trenin, "Why the Reset Should Be Reset," *New York Times* (12 December 2012); and Shleifer and Treisman, "Why Moscow Says No."

[96] Blank, "Introduction," 16.

States and Russia is absolutely critical to world peace and stability."[97] Similarly, the 2010 NATO Strategic Concept affirmed that "NATO–Russia cooperation is of strategic importance as it contributes to creating a common space of peace, stability and security…. [W]e remain convinced that the security of NATO and Russia is intertwined and that a strong and constructive partnership based on mutual confidence, transparency and predictability can best serve our security."[98] Russia, for its part, has taken a more cautious view, calling in its national security strategy for "an equitable and valuable strategic partnership with the United States of America, on the basis of shared interests and taking into account the key influence of Russian-American relations on the international situation as a whole" and indicating its willingness to "develop relations with NATO on the basis of equality and in the interests of strengthening the general security of the Euro-Atlantic region."[99]

Unfortunately, the current strategic dialogue is limited, both with respect to what issues are being discussed and in terms of concrete progress anywhere on the agenda. The U.S., Russia, and NATO all suffer from myopia in their views of engagement, tackling only a narrow range of issues, declining to take risks to achieve success, and thereby missing opportunities to score even minor victories.[100] This failure is disappointing, because cooperation for its own sake is fruitful as it breaks the inertia of intractability and breeds further cooperation, whether on related issues or elsewhere on the docket.[101] Tangible progress is elusive, and finding a way to achieve it must be the goal, starting with small wins, building confidence, making cooperation a habit, and ultimately taking on the most demanding tasks as trusted partners. For this reason, in an open letter published earlier this year, four former U.S. Ambassadors to Moscow and four former Soviet or Russian Ambassadors to Washington chided their current governments to work harder in this regard because "a more active search for joint projects in areas of mutual self-interest will add an important element to the structure of Russian-American stability."[102] Cybersecurity represents one key area where U.S., NATO, and Russian interests

[97] Barack Obama and Dmitry Medvedev, "Remarks by President Obama and President Medvedev of Russia After Bilateral Meeting," 26 March 2012.; available at www.whitehouse.gov/the-press-office/2012/03/26/remarks-president-obama-and-president-medvedev-russia-after-bilateral-me.

[98] North Atlantic Treaty Organization, *Active Engagement, Modern Defence* (Strategic Concept), 29–30.

[99] National Security Council of the Russian Federation. "Russia's National Security Strategy to 2020," 12 May 2009; available at http://rustrans.wikidot.com/russia-s-national-security-strategy-to-2020 (English translation).

[100] Blank, "Introduction," 17; Oliker, et al., *Russian Foreign Policy*, 137; Sestanovich, "Reassessing the U.S.-Russia 'Reset'."

[101] Blank, "Introduction," 6.

[102] John Beyrle, et al. "Priorities for Russia-U.S. Relations: A Statement by Former Ambassadors to Washington and Moscow," Carnegie Endowment for International Peace Web Site (12 April 2013); available at http://carnegieendowment.org/2013/04/12/priorities-for-russia-u.s.-relations-statement-by-former-ambassadors-to-washington-and-moscow/fza1.

coincide and rapid progress is eminently achievable, providing a foundation for further collaboration and improving the broader relationships among all parties in the process.

Russia and Cybersecurity

Russia is a highly capable power in the cyber realm, described by the head of U.S. Cyber Command as a "near peer" to the U.S.,[103] with more sophistication than other advanced competitors like China and Israel.[104] This aptitude is a consequence of Russia's wealth of highly educated workers with strong technical backgrounds, who make up a large pool of skilled human capital well suited for employment on information technology endeavors.[105] Lacking outlets for this talent in the underdeveloped Russian tech industry, Russian government and organized crime networks—which appear to have a great deal of overlap in the cyber realm[106]—provide the largest markets for gainful employment.[107]

Although Russia possesses an advanced capability that ranks among the best in the world, its fundamental understanding of cybersecurity diverges widely from that of the U.S. and NATO,[108] which creates philosophical and conceptual differences that pose real—albeit surmountable—obstacles to constructive dialogue on cyber issues. At present, a lack of common understanding makes any discussion between Russia and the West on cyber topics, in the words of one expert, an act of "mutual incomprehension and apparent intransigence."[109] These differences must be understood and resolved for cooperation to bear fruit, which can only be achieved through regular dialogue and consistent interaction, a perspective reflected in the comment by the U.S. Secretary of State's Coordinator for Cyber Issues Christopher Painter that "We need to engage with countries around the world, even with those with whom we disagree."[110]

[103] Keir Giles, "'Information Troops' – A Russian Cyber Command?" in *3rd International Conference on Cyber Conflict*, ed. Christian Czosseck, Enn Tyugu, and Thomas Wingfield (Tallinn: CCD COE Publications, 2011), 50.

[104] James Fallows, "Cyber Warriors," *The Atlantic* (March 2010); available at www.theatlantic.com/magazine/archive/2010/03/cyber-warriors/307917/. See also David A. Fulghum, "China Cyber-skills Are Improving But Still Don't Top Russia and Israel," *Aviation Week* (28 March 2012).

[105] Flook, "Russia and the Cyber Threat"; Fulghum, "China Cyber-skills Are Improving."

[106] Carr, *Inside Cyber Warfare*, 124–25; Flook, "Russia and the Cyber Threat"; Joshua McGee, "US-Russia Diplomacy – The "Reset" of Relations in Cyberspace," Center for Strategic and International Studies Web Site (5 August 2011); available at http://csis.org/blog/us-russia-diplomacy-reset-relations-cyberspace.

[107] Flook, "Russia and the Cyber Threat"; "Interview with Joseph Menn, Author of Fatal System Error," *Cyveillance* (2 June 2010); available at https://blog.cyveillance.com/general-cyberintel/fatal-system-error-joseph-menn.

[108] Jason Healey, "Comparing Norms for National Conduct in Cyberspace," *New Atlanticist* (20 June 2011); available at www.acus.org/new_atlanticist/comparing-norms-national-conduct-cyberspace.

[109] Giles, "Russia's Public Stance on Cyberspace Issues," 64.

[110] Benjamin Boudreaux, "Cyber Diplomats," *State Magazine* (April 2013): 32.

Russia does not see cybersecurity or any cyber activity as a distinct issue, standing alone and addressed in isolation, as is the tendency in the West. In fact, *cyber*—a ubiquitous term in the West—is not a word used in official Russian-language documents, except when referring to the activities of other countries. Rather, where Westerners discuss *cyber,* the Russian military community instead prefers to use the term *informationization*, viewing cyber as an embedded part of the broader concept of information operations.[111] Indeed, the foundational document for Russian information security does not contain either the words *cyber* or *Internet* anywhere in its text.[112] Rather, the Russians take a holistic, integrated approach to information operations (or information warfare) that blends a technical dimension consisting of hardware, software, and other technological components with a psychological aspect that affects information processing, perceptions, attitudes, and decisions to provide Russia an information advantage over competitors or adversaries.[113] In the Russian view, the technical dimension of cyber—protecting data and computer systems from hackers, spies, and criminals—cannot be divorced from the cognitive aspects of employing information, such as public affairs, psychological operations, deception, and so on.[114]

This point of view leads Russia to focus its national information security efforts on protecting society from "harmful" information. The notion that information might be considered dangerous highlights another important distinction between Russian and Western perspectives. The West sees information as a public good, which governments should subject to minimal controls and allow to flow as freely as possible, including over the Internet – what former U.S. Secretary of State Hillary Clinton called the "freedom to connect."[115] In contrast, the Russian Federation worries heavily about the unfettered exchange of information having a destabilizing effect on its societies, or at least on the rule of the current leadership.[116] "Internet sovereignty," or the ability of the government to monitor and, if necessary, control the information domain is an essential element of the Russian position on cybersecurity and a key component of Russia's international

[111] Timothy Thomas, "Nation-State Cyber Strategies: Examples from China and Russia," in *Cyberpower and National Security,* ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, D.C.: National Defense University Press, 2009), 476.

[112] "Information Security Doctrine of the Russian Federation" 9 September 2000; available at www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument.

[113] Timothy Thomas, *Recasting the Red Star: Russia Forges Tradition and Technology Through Toughness* (Fort Leavenworth, KS: Foreign Military Studies Office, 2011), 137–52.

[114] Thomas, "Nation-State Cyber Strategies," 477–79.

[115] Hillary Clinton, "Remarks on Internet Freedom," 21 January 2010; available at www.state.gov/secretary/rm/2010/01/135519.htm

[116] Jason Healey, "Breakthrough or Just Broken? China and Russia's UNGA Proposal on Cyber Norms," *New Atlanticist* (21 September 2011); available at www.atlanticcouncil.org/blogs/new-atlanticist/breakthrough-or-just-broken-china-and-russia-s-unga-proposal-on-cyber-norms.

efforts on cyber issues to date.[117] It also remains an important point of disagreement with the U.S. and other mature democracies.

In the international arena, the one important treaty on cybersecurity issues already in existence is the Council of Europe's Convention on Cybercrime, also known as the Budapest Convention, a major regional agreement with the potential for global acceptance. It has been adopted by thirty-nine mostly European countries—including the U.S. but not Russia—since its initiation in 2001.[118] The treaty provides a model for cooperation between different countries and with private industry in combating cybercrime, offering a template with potential for expansion to other cyber issues.[119] Russia, however, objects to ratification of the treaty as an infringement of its sovereignty, as it would invite demands for cooperation in identifying, for example, the perpetrators of the cyber attacks on Estonia in 2007 or Georgia in 2008, along with requests from foreign law enforcement agencies in shutting down the extensive cybercriminal activity that originates on Russia territory.[120]

Rather than support the Budapest Convention, Russia has emphasized the need for a new international regime that more closely corresponds to its views on cybersecurity. Russian officials and academics consistently espouse a position that existing international law is inadequate and that new accords are necessary to affirm national sovereignty and deter aggressive behavior in cyberspace.[121] Their proposals, including the 2011 letter to the UN Secretary-General it co-authored with China, Tajikistan, and Uzbekistan, generally seem to share three aims: to constrain or limit competing U.S. initiatives to develop norms in cyberspace, which they view as a means of consolidating the U.S. competitive advantage in cyberspace; to affirm the rights of countries to monitor and control the flow of information over the Internet, which they see as essential to ensuring domestic security; and to prevent the further development or proliferation of offensive cyber weapons. These tenets contrast sharply with the Western emphasis on commitment to the free flow of information, measures to combat cyber crime, and state responsibility for Internet activity occurring within a country's borders.[122] These differences might appear to be irreconcilable at first blush, limiting the odds of achieving consensus on an international framework for cyber operations.[123] However, there are many points of agreement that provide a starting point for cooperation – on securing supply

[117] Giles, "Russian Cyber Security," 2.

[118] Council of Europe, "Convention on Cybercrime, Chart of Signatures and Ratifications," 22 March 2013; available at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM =&DF=&CL=ENG.

[119] Hughes, "A Treaty for Cyberspace," 534.

[120] Giles, "'Information Troops'," 51; Giles, "Russia's Public Stance on Cyberspace Issues," 67.

[121] Dmitry I. Grigoriev, "Russian Priorities and Steps Towards Cybersecurity," in *Global Cyber Deterrence: Views of China, the U.S., Russia, India and Norway*, ed. Andrew Nagorski (New York: EastWest Institute, 2010).

[122] Carr, *Inside Cyber Warfare*, 34–35; Healey, "Breakthrough or Just Broken?"

[123] Shane Harris, "The Cyberwar Plan," *National Journal* (14 November 2009).

chains, protecting critical infrastructure, sharing information on threats, and combating Internet use by drug traffickers and pedophiles.[124]

While Russia may view cybersecurity differently from the U.S. and its NATO partners, taking advantage of the commonalities that do exist is necessary in order to forge a broader agenda on cybersecurity, across the spectrum of security issues and, ultimately, beyond mere security to a fuller range of topics. Expanding the "envelope of cooperation" demands innovative partnering, breaking patterns of mistrust, and forging new means to identify and achieve common goals.[125] In the context of U.S.–Russia and NATO–Russia relations, this will involve reconciling the lack of U.S. and NATO trust in Russia, as well as ensuring that Russia feels like an equal partner, fully vested in the ownership and decision making of whatever venues are used for engagement. It will also require working through seemingly incompatible visions for European security, dissimilar strategic cultures, and a track record startlingly lacking in sustained tangible co-operation.[126] Both sides will have to be willing to take some risks, both in security terms and with domestic constituencies, to achieve appreciable results.[127] But such risks are a modest investment that offers the potential of substantial return on cybersecurity issues of great importance to all parties.[128]

Engaging Russia in the Cyber Domain

The U.S. and Russia have long acknowledged their mutual interest in cooperating on cybersecurity issues, stretching back to a 1998 declaration by U.S. President Bill Clinton and Russian President Boris Yeltsin that included a commitment to "mitigating the negative aspects of the information technology revolution," which they characterized as a "serious challenge" to the security of the two countries.[129] The same statement also emphasized collaboration in anticipation of Y2K,[130] which resulted in extensive joint preparations for and monitoring of potential information technology problems at the turn of the millennium.[131] Since then, the two countries have worked together primarily on is-

[124] Healey, "Breakthrough or Just Broken?"; "Russian Premier Chides USA over 'Unfair' Internet Policy, Urges 'Common Rules'," *Interfax* (30 October 2012); available at www.accessmylibrary.com/article-1G1-306951274/russian-premier-chides-usa.html.

[125] Martin E. Dempsey, "From the Chairman: Making Strategy Work," *Joint Forces Quarterly* 66 (2012): 2–3.

[126] James Sherr, "NATO and Russia: Doomed to Disappointment?" *NATO Review 2011*; available at www.nato.int/docu/review/2011/nato_russia/Disappointment/EN/index.htm.

[127] Oliker, et al., *Russian Foreign Policy*, 138.

[128] Dempsey, "From the Chairman: Making Strategy Work," 2–3.

[129] "Joint Statement on Common Security Challenges at the Threshold of the Twenty-First Century," 2 September 1998; available at http://www.gpo.gov/fdsys/pkg/WCPD-1998-09-07/pdf/WCPD-1998-09-07-Pg1696.pdf.

[130] Ibid.

[131] Among many others, see for example Stephen Barr, "U.S., Russia Agree to Establish Y2K Center," *Washington Post* (11 September 1999); Elizabeth Becker, "U.S. and Russia Agree on Joint Defense Against Y2K Debacles," *New York Times* (28 October 1999); Tom Bowman,

sues tangentially related to cybersecurity, such as joint monitoring of electronic launch procedures for ballistic missiles and updated digital encryption standards for the White House–Kremlin hotline.[132] In December 2009, the U.S. and Russia affirmed their commitment to cooperation during a meeting of the UN Committee on Disarmament and International Security by agreeing to bolster Internet security and develop norms for military operations in cyberspace.[133] Shortly afterward, this led to a UN General Assembly Resolution calling for the "strengthening the security of global information and telecommunications systems" and "study [of] existing and potential threats in the sphere of information security and possible cooperative measures to address them."[134] U.S.–Russian concurrence on the resolution's wording—however vague and seemingly anodyne the content—represented a breakthrough in bilateral cyber diplomacy, ending ten previous years of wrangling over verbiage and leading to further official discussions on cybersecurity.[135]

Most subsequent official bilateral consultations have been held deliberately out of the public view, and have been described by U.S. Vice President Joseph Biden as designed to "build up cooperation and to set up lines of communication in the event of an alarming incident."[136] The latest series of talks, which began in February 2011, focused on cybersecurity areas of mutual concern such as exchanging technical information on threats, working toward common understanding on military operations in cyberspace, and establishing protocols for communicating between Moscow and Washington during cyber-related crises.[137] In an early gesture that suggested a symbolic effort to build trust, the U.S. complied with a proposal to exchange position papers on cyberspace by providing the Russians with the Pentagon's *Strategy for Operating in Cyberspace*[138] before

"U.S., Russian Military Ally Against Y2K Bug," *Baltimore Sun* (27 October 1999); and Elizabeth Shogren, "U.S., Russia Cooperate on Y2K Concerns," *Los Angeles Times* (2 December 1999).

[132] Franz-Stefan Gady and Greg Austin, *Russia, the United States, and Cyber Diplomacy* (New York City: EastWest Institute, 2010), i.

[133] Ibid.

[134] United Nations, "Developments in the Field of Information and Telecommunications in the Context of International Security," United Nations General Assembly, A/Res/64/25 (2 December 2009).

[135] Gady and Austin, *Russia, the United States, and Cyber Diplomacy*, 3–4.

[136] Ellen Nakashima, "In U.S.-Russia Deal, Nuclear Communication System May Be Used for Cybersecurity," *Washington Post* (26 April 2012).

[137] Howard Schmidt, "U.S. and Russia: Expanding the "Reset" to Cyberspace," The White House Blog (12 July 2011); available at http://www.whitehouse.gov/blog/2011/07/12/us-and-russia-expanding-reset-cyberspace. See also Barack Obama and Vladmir Putin, "Joint Statement by the Presidents of the United States of America and the Russian Federation on a New Field of Cooperation in Confidence Building," 17 June 2013; available at www.whitehouse.gov/the-press-office/2013/06/17/joint-statement-presidents-united-states-america-and-russian-federatio-0.

[138] United States Department of Defense, *Strategy for Operating in Cyberspace.*

the document was officially published in July 2011.[139] U.S. Cybersecurity Coordinator Howard Schmidt and Russian National Security Council Deputy Secretary Nikolay Klimashin issued a joint statement in June 2011 characterizing the discussions as "deepening mutual understanding on national security issues in cyberspace,"[140] and Schmidt later blogged that they are "a prime example of the 'Reset' in U.S.–Russia relations taking on a new and important dimension."[141]

More than two years of these talks culminated in a bilateral accord announced by U.S. President Obama and Russian President Putin in June 2013 on the sidelines of the G8 Summit in Northern Ireland. As expected, the joint statement issued by the White House described measures including information sharing between national computer emergency response teams (CERTs), expansion of the nuclear hotline to provide direct communications during cyber crises, and establishment of a cybersecurity working group within the framework of the U.S.–Russia Bilateral Presidential Commission. Although the announcement rightly calls U.S.–Russian cybersecurity cooperation "essential to safeguarding the security of our countries" and describes the agreement as "landmark steps" in helping "to meet our national and broader international interests," much work remains to be done. Mere willingness to cooperate signals the importance of cybersecurity to both parties—especially in light of the general contentiousness of U.S.–Russian relations—but the pact should be seen as a cautious but necessary first step in a deepening relationship rather than an end in itself.[142]

NATO and Russia have to date shared a relationship on cybersecurity issues that is even less auspicious. The transition from Cold War adversaries to modern partners has been halting and is still incomplete. Writ large, NATO–Russia relations are governed by the 1997 NATO–Russia Founding Act on Mutual Relations, Cooperation, and Security, which established relations on a "NATO+1" basis, meaning that NATO would act as a bloc in working bilaterally with Russia on any issue. In 2002, the Rome Declaration modified that relationship by establishing the NATO–Russia Council (NRC) as a forum for Russia to ostensibly meet as an equal partner of the NATO member states in addressing areas of common interest.[143] Since then, Russia has made repeated overtures in the NRC to cooperate on cybersecurity, but NATO has never demonstrated the willingness—i.e., the trust—to accept. During the 2012 NATO–Russia Council meeting of foreign ministers, the strongest endorsement that the parties could muster was "interest expressed in exchanging views on cybersecurity and in discussing opportunities for mili-

[139] Nakashima, "In U.S.-Russia Deal."

[140] "Joint Statement by Cybersecurity Coordinator Schmidt and Deputy Secretary Klimashin: U.S. and Russian Delegations Meet to Discuss Confidence-Building Measures in Cyberspace," 23 June 2011; available at www.whitehouse.gov/sites/default/files/uploads/2011_klimashin_schmidt_cyber_joint_statement.pdf.

[141] Schmidt, "U.S. and Russia: Expanding the "Reset" to Cyberspace."

[142] Obama and Putin, "Joint Statement by the Presidents of the United States and Russia."

[143] NATO–Russia Council, "About NRC," NATO-Russia Council Web Site (2013); available at www.nato-russia-council.info/en/about/.

tary-technical cooperation," hardly a clarion call for a true partnership.[144] Most recently, Russian Foreign Minister Sergey Lavrov called for Russia and NATO to work together to build up cybersecurity during the April 2013 NATO–Russia Council meeting of foreign ministers, and Lavrov later told the media that U.S. Secretary of State John Kerry had "immediately supported" the proposal, although no official U.S. or NATO statement on Lavrov's proposal followed the meetings.[145]

As with all Alliance decisions, achieving unanimity among the twenty-eight member nations is extremely difficult. Any interaction with Russia is a special challenge given the sensitivity of several current NATO countries that were either former Warsaw Pact members or Soviet republics and view their relations with Russia during the Soviet era through a lens of domination or even occupation. For them, discussions of general partnership with Russia verge on heresy, and cooperation on cybersecurity, particularly in the wake of the 2007 cyber attacks on Estonia and the 2008 Russia-Georgia War, is nearly unthinkable. Fortunately for the skittish NATO members—or, perhaps more appropriately, because without their consent, no change is possible—NATO policy essentially forbids cooperating on cybersecurity with any countries outside the Alliance except for a select group of its closest partners, requiring either a change to current policy or case-by-case exceptions to forge any real cyber partnership.[146]

An Agenda for NATO–Russian Cooperation

Absent any ongoing cooperation between NATO and Russia, a virtually blank slate exists for developing NATO's agenda to finally begin to engage Russia in the cyber domain – and NATO must acknowledge that such engagement is imperative going forward. While the NATO Policy on Cyber Defense acknowledges that NATO will "tailor its international engagement based on shared values and common approaches,"[147] and a recent NATO study called international partners "essential actors of NATO's cyber defense" with whom NATO should "develop bilateral arrangements … focusing on infor-

[144] North Atlantic Treaty Organization, Press Release (2012) 053, "Meeting of the NATO-Russia Council at the Level of Foreign Ministers Held in Brussels on 19 April 2012," 19 April 2012; available at www.nato.int/cps/en/natolive/official_texts_86211.htm?mode=pressrelease.

[145] Sergey Lavrov, "Speech of and Answers to Questions of Mass Media by Russian Foreign Minister Sergey Lavrov Summarizing the Results of the Session of NATO-Russia Council at the Foreign Minister Level, Brussels, 23 April 2013," Ministry of Foreign Affairs of the Russian Federation Official Site, 23 April 2013; available at www.mid.ru/BDOMP//brp_4.nsf/english/EFF6D7ADFD1A258B44257B58004CF50C.

[146] NATO's menu of partnership programs is complex and, in theory, each partner country has its own Individual Partnership and Cooperation Program with NATO, which may or may not include cybersecurity cooperation. In practice, seven non-NATO nations have comprehensive cooperation agreements for cybersecurity in place according to Gerhard Jandl, "The Challenges of Cyber Security – A Government's Perspective," *Human Security Perspectives* (2012): 26–37. See North Atlantic Treaty Organization, "Partnership Tools" for additional details on NATO partnership policy; available at www.nato.int/cps/en/natolive/topics_80925.htm.

[147] North Atlantic Treaty Organization, "Defending the Networks."

mation-sharing, exchange of best practices, and judicial agreements," Alliance gridlock has prevented NATO from even initiating a relationship with Russia on issues of mutual concern.[148] As a consequence, NATO members with favorable bilateral relations with the Russian Federation are bypassing NATO to work directly with Russia on cybersecurity and other topics, which neutralizes the collective influence of NATO and plays toward the Russian strategic goal of marginalizing NATO wherever possible.[149] Rather than sitting on the sidelines as the cyber domain is evolving around it, NATO has the opportunity and the need now to match its actions to its rhetoric by accepting Russian overtures to cooperate on cybersecurity. It should build internal consensus on engaging Russia with relatively low-cost, low-risk measures where both sides can easily find agreement as first steps toward an eventually more substantial partnership that tackles the thornier problems where the two sides have fundamental differences. Specifically, NATO should seek to cooperate with Russia to accomplish the following goals.

Add a Cybersecurity Working Group to the NATO-Russia Council. Ideally, this arrangement would establish a stand-alone working group on par with working groups covering topics like missile defense, logistics, or terrorism. If that were to provide too broad of a mandate for the Alliance partners to agree to, it could be formed as a subgroup underneath the Science for Peace and Security Committee with a much narrower and more technical purview. In any case, forming a working group at the NRC would signal the intention to work seriously with Russia on cybersecurity and would provide an organizational venue for doing so.[150]

Partner Computer Emergency Response Teams. Regardless of the level of trust between NATO and the Russian Federation, having contacts established between the technical experts who have the ability to respond in the event of a crisis is invaluable.[151] NATO should collectively adopt the pragmatic stance of some of its member states and begin a series of limited, technically-oriented exchanges between the NATO Computer Incident Response Capability Technical Center and the Russian CERT in order to exchange technical information and determine how best to communicate during a crisis.

[148] Vincent Joubert, *Five Years after Estonia's Cyber Attacks: Lessons Learned for NATO,* NATO Defense College Research Paper No. 76 (Rome: Imprimerie Deltamedia Group, 2012), 7.

[149] Haider Ali Hussein Mullick, "Catching the BUG (Belarus, Ukraine and Georgia) – Russia's Buffer or NATO's Annex? A New Framework for Euro-Atlantic-Russian Cooperation," *Georgetown Journal of International Affairs* (4 May 2013); available at http://journal.georgetown.edu/2013/05/04/catching-the-bug-belarus-ukraine-and-georgia-russias-buffer-or-natos-annex-a-new-framework-for-euro-atlantic-russian-cooperation-by-haider-ali-hussein-mullick/.

[150] NATO-Russia Council, "About NRC."

[151] "Joint Statement on Bilateral Discussions on Cooperation in Cybersecurity, China Institute of International Relations (CICIR)–Center for Strategic and International Studies (CSIS)," Center for Strategic and International Studies (June 2012); available at http://csis.org/files/attachments/120615_JointStatement_CICIR.pdf.

Share Cyber Intel. Because cyberspace is constantly evolving and the nefarious actors who operate within it are continually adapting, maintaining up-to-date information on cyber threats is an endless challenge. Likewise, sharing intelligence across NATO can be a sensitive and difficult process, so any proposal for trading secrets with Russia might on the surface seem dubious – except that during an April 2013 visit to Moscow, NATO Deputy Secretary-General Alexander Vershbow proposed the creation of two centers to allow Russia and NATO to share intelligence, conduct joint planning, and coordinate operations on missile defense.[152] While a final agreement on establishing these centers is nowhere near, missile defense has been as much of a source of friction between the U.S., NATO, and Russia as cybersecurity, so the proposed facilities provide a template for a cyber threat information clearinghouse as another space for NATO and Russia to cooperate. Such a clearinghouse could start small and work initially on shared analysis of excellent but unclassified data from commercial cybersecurity firms and, as trust is built, graduate to more sensitive and classified intelligence products.[153]

Develop Confidence-Building Measures. The Organization for Security and Cooperation in Europe (OSCE) is nearing completion of a set of confidence-building measures (CBMs) intended to prevent misunderstandings and avert international conflicts among its fifty-seven member countries.[154] Although the publicly available draft of the measures reveals them to be voluntary and not particularly robust,[155] the agreement, once finalized, will be important for having started a conversation on cybersecurity among over a quarter of the world's nation-states and in facilitating the exchange of cybersecurity terminology, doctrine, and contacts among the members. NATO should build on the OSCE agenda to pursue a more detailed and more ambitious set of CBMs with Russia, including joint early-warning mechanisms, exchanges of technical cybersecurity recommendations, and improvement of cyber crisis communication channels.[156] Given that all twenty-eight NATO countries and Russia are part of the OSCE, achieving

[152] Inna Soboleva, "NATO, Russia Consider Joint Missile-Defense System," *Russia Beyond the Headlines* (8 April 2013); available at http://rbth.ru/politics/2013/04/08/nato_russia_consider_joint_missile-defense_system_24761.html.

[153] Mandiant Intel Team, "No Clearance Required: Using Commercial Threat Intelligence in the Federal Space," Mandiant Web Site (2 May 2013); available at www.mandiant.com/blog/clearance-required-commercial-threat-intelligence-federal-space/.

[154] Aliya Sternstein, "U.S., Russia, Other Nations Near Agreement on Cyber Early-Warning Pact," *Nextgov* (5 December 2012); available at www.nextgov.com/cybersecurity/2012/12/us-russia-other-nations-near-agreement-cyber-early-warning-pact/59977/.

[155] Jeffrey Carr, "OSCE's Cyber Security Confidence Building Measures Revealed by Anonymous," *Digital Dao* (13 November 2012); available at http://jeffreycarr.blogspot.de/2012/11/osces-cyber-security-confidence.html#!/2012/11/osces-cyber-security-confidence.html. The hacker group Anonymous stole a confidential draft of the CBMs from the OSCE Internet server on 11 November 2012, and posted the documents online. Carr's blog provides a summary and analysis of the contents, along with a link to the stolen documents.

[156] Detlev Wolter, "Looking towards the Future of Cyber Security: What Does a Stable Cyber Environment Look Like?" Speech at the UNIDIR Cyber Security Conference 2012 (8 November 2012); available at www.unidir.ch/files/conferences/pdfs/pdf-conf1920.pdf.

consensus on confidence-building measures at the NRC should be attainable, and it would go a long way to addressing Russia's almost paralyzing fears of being blamed for a cyber incident in which it legitimately played no role.[157] And since NATO and Russia have a long track record of devising CBMs related to nuclear weapons, adapting those existing procedures and processes to cybersecurity would appear eminently achievable.

Conduct Combined Cyber Defense Exercises. Concerns about allowing Russian participation in cyber exercises abound—both objections to any Russian role and wariness over Russian intimidation of other exercise partners, especially those from the post-Soviet space—but NATO has been successfully dealing with Moscow in non-cyber contexts for years. NATO should adopt a similar approach with cybersecurity. Since 2010, U.S. European Command (EUCOM) has hosted a series of cyber defense exercises called Cyber Endeavor, nested in and simultaneous with its larger Combined Endeavor command-and-control exercise.[158] Because the EUCOM commander is dual-hatted as the NATO Supreme Allied Commander, this arrangement allows all of NATO to participate in the exercise, along with other nations that fall outside of NATO's cybersecurity cooperation policy, effectively sidestepping the NATO guidelines and expanding the circle of authorized participants. In 2012, the exercise included 175 participants from thirty-two countries, some members of NATO and some not, focused on network defense procedures and cyber incident response.[159] NATO should embrace this forum for engaging Russia by inviting it, through EUCOM, to future iterations of this exercise, initially as an observer and later as a full participant, as it has done on other, non-cyber exercises in recent years.[160]

NATO also has conducted an annual, more limited, technical cyber defense exercise series called Locked Shields through the Cooperative Cyber Defense Center of Excellence (CCD COE) in Tallinn, Estonia. The 2013 exercise included CERTs from NATO headquarters, eight NATO member countries, and Finland (one of the countries NATO security policy allows the Alliance to partner with on cybersecurity issues) in a real-time network defense exercise focused on mitigating large-scale cyber attacks.[161] Although the current security policy proscribes Russian participation, the CCD COE Steering

[157] This situation, commonly referred to as a "false flag," is described in, among other sources, in Geers, *Strategic Cyber Security*, 118; and Nye, *Cyber Power,* 16–17. It was also a consistent theme of nearly every Russian speaker at the 7th International Forum for Partnership of State Authorities, Civil Society, and the Business Community in Ensuring International Information Security, held 22–25 April 2013, in Garmisch-Partenkirchen, Germany.

[158] "Exercise Combined Endeavor."

[159] James G. Stavridis, Testimony before the 113th Congress, House and Senate Armed Services Committee Testimony, 19 March 2013; available at www.armed-services.senate.gov/statemnt/2013/03%20March/Stavridis%2003-19-13.pdf, 13.

[160] James G. Stavridis, Testimony before the 112th Congress, House and Senate Armed Services Committee Testimony, 20 March 2011; available at www.armed-services.senate.gov/statemnt/2011/03%20March/ Stavridis%2003-29-11.pdf, 17.

[161] CCD COE, "NATO Team Wins the Locked Shields Cyber Defence Exercise," NATO Cooperative Cyber Defense Centre of Excellence Web Site (26 April 2013); available at www.ccdcoe.org/413.html.

Committee should ask its stakeholders for explicit permission to pursue Russian involvement in Locked Shields, first as an observer and then as a participant, perhaps partnered with another CERT.

Forge Consensus on International Cyber Law. The fundamental disagreement on the adequacy of existing international law—the U.S. and NATO want to apply current law to cyber issues, while Russia insists that a new international treaty is required—seriously inhibits progress on other cyber issues, because the law defines what is and is not permissible in cyberspace. As a first step toward resolving these differences, NATO should involve Russia in its efforts to interpret and elaborate international cyber law, which could help soften the divide that exists between the two camps.

An easy, low-risk first step is to invite Russian participants to the semi-annual International Law of Cyber Operations Course, organized by the CCD COE, the U.S. Naval War College, and the NATO School. The course is intended for legal advisors to cyber policymakers and provides a basic knowledge of international law as it applies to cyber operations. It could serve as a valuable forum for thoughtful interaction between legal experts from NATO and Russia.[162]

NATO also needs to recognize the opportunity it missed in sponsoring the development of the Tallinn Manual with virtually no representation or input provided by experts from Russia or virtually anywhere outside of Western Europe or North America, which resulted in a legal reference that essentially proselytizes to the already converted on international cyber law. As a consequence, Russia has adopted a position that either ignores or rejects (depending on the source) the interpretations of international law represented in the Tallinn Manual.[163] Future projects of this nature are important, but their impacts will be limited as long as the pool of contributors remains exclusive, as is the plan for a follow-up Tallinn 2.0 project to examine international law for cyber attacks that stay below the threshold of armed attack.[164] Admittedly, finding a Russian legal expert with the appropriate credentials who would be a constructive participant and not an obstacle to progress could prove difficult. However, when the alternative is to create another reference work that "[l]arge parts of the world will not consider … legitimate,"[165] NATO should underwrite more inclusive projects that are likelier to find widespread acceptance and narrow the differences between the opposing viewpoints on key issues of international cyber law.

[162] CCD COE, "International Law of Cyber Operations," NATO Cooperative Cyber Defense Centre of Excellence Web Site; available at www.ccdcoe.org/352.html.

[163] "The Applicability of International Law in Cyberspace – From If to How?" Panel Three at the Georgetown University Conference on the International Law on Cyber (10 April 2013); available at http://lsgs.georgetown.edu/events/InternationalEngagementonCyber2013/PanelThreeApplicabilityofInternationalLawinCyberspace041013.pdf. The comments of Dr. Anatoly Streltsov from Lomonosov Moscow State University in this transcript are representative.

[164] CCD COE, "Four Legal Experts Appointed as Centre's Senior Fellows," NATO Cooperative Cyber Defense Centre of Excellence Web Site (9 May 2013); available at www.ccdcoe.org/422.html.

[165] "Apply International Law to Cyber-Warfare? Good Luck," *The Economist* (23 March 2013).

U.S.–Russia Cybersecurity Engagement

Whereas NATO–Russian cyber cooperation is essentially nonexistent, U.S.–Russian bilateral cyber cooperation can best be characterized as nascent and low-key, even if the June 2013 breakthrough agreement on cybersecurity cooperation is viewed in an optimistic light. Although the 2011 U.S. *International Strategy for Cyberspace* calls for a "wide range of bilateral dialogues" to "advance common action on cyberspace's emerging challenges,"[166] publicly very little information is available about work with Russia on any cybersecurity issues beyond occasional media reports of law enforcement assistance in bringing down an Internet fraud ring.[167] New cooperation between the U.S. and Russia on cyber issues may result from the June 2013 accord, but the modest measures it contained are more token steps that indicate a desire to work together than they are deeply substantive solutions to the most pressing cybersecurity challenges the two countries face. The establishment of a cyber working group under the auspices of the U.S.–Russia Presidential Commission provides a forum for the two sides to maintain momentum toward further cooperation. Indeed, the U.S. and Russia should build on their recent achievement to solidify their relationship in cyberspace by pursuing the following steps.

Deepening CERT Partnerships. Whatever increase in interaction has taken place between U.S. and Russian CERTs that has occurred since the Obama-Putin announcement on cybersecurity cooperation has happened behind closed doors – and it has almost certainly not been enough. As with NATO–Russian CERT partnerships, the value of knowing who to call in the event of a crisis is immeasurable, and increasing the frequency of interaction between U.S. and Russian CERTs has virtually zero downside. Over time, the two sides should strive for increased real-time collaboration between technical experts and analysts, joint technical training and exchanges, sharing of information on threats and trends, and development of standardized incident response management procedures to build trust and confidence between the two teams and to increase their interoperability during crises.

Conducting Combined Cyber Defense Exercises. The U.S. should invite Russia to begin participating in its European Command-sponsored exercise Cyber Endeavor, which would be important for both direct engagement with Russia and to boost NATO's involvement with Russia on cyber defense cooperation. At the same time, U.S. Pacific Command also hosts its own annual Cyber Endeavor exercise, which in 2012 involved

[166] Office of the President of the United States, *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World* (Washington, D.C.: Government Printing Office, 2011), 12.

[167] Nikola Krastev, "In U.S. Cybercrime Case, Track Record Indicates Russia Willing to Cooperate," *Radio Free Europe/Radio Liberty* (9 October 2010); available at www.rferl.org/content/In_US_Cybercrime_Case_Track_Record_Indicates_Russia_Willing_To_Cooperate/2185564.html.

twenty-two countries from the Asia-Pacific region.[168] Because none of the PACOM exercise participants are former Soviet republics or Warsaw Pact countries, Russian involvement would likely produce less controversy than it would in the European theater. The U.S. should extend invitations to the Russian Federation to both Cyber Endeavor exercises, starting as an observer and with the intent to bring it up to full participation as soon as possible. It should also work to include cyber defense dimensions to ongoing U.S.–Russian exercises like Northern Eagle, Atlas Vision, and Vigilant Eagle to improve cyber defense interoperability between the two militaries at all levels.[169]

Cooperating on Cybercrime. U.S.–Russian cooperation on cybercrime has been sporadic, while the growth of organized Russian cybercriminal networks has continued unabated in recent years, accounting for 36 percent of global cybercrime in 2011 in spite of reported Russian government efforts to crack down.[170] The ideal outcome for the U.S. would be to convince Russia to adopt the Budapest Convention, which appears unlikely given Russia's clamorous opposition on grounds of sovereignty. The U.S. should continue to press Russia to adopt the Budapest Convention, but it should not abandon its efforts to improve cooperation with Russia on combating cybercrime through the G8's Roma-Lyon High Tech Crime Sub-Group, which has produced a small but substantive program of law enforcement cooperation.[171] The U.S. should also encourage Russia's inclusion in programs that combat types of online crime where Russia has publicly advocated for increased cooperation and whose subject makes controversy unlikely, such as fighting child pornography or drug trafficking.[172] More directly, the U.S. should work to strengthen its bilateral law enforcement cooperation on cyber issues, capitalizing on the recent progress in the wake of the Boston Marathon bombings,[173] to cement its relation-

[168] Carl Hudson, "Pacific Endeavor 2012 Begins," United States Pacific Command Web Site (8 August 2012); available at www.pacom.mil/media/news/2012/08/08-pacific-endeavor-2012-begins.shtml.

[169] Gerald O'Dwyer, "Norway Hails Northern Eagle as Bridge-Builder," *DefenseNews* (24 August 2012); available at www.defensenews.com/article/20120824/DEFREG01/308240002/Norway-Hails-Northern-Eagle-Bridge-builder. See also "Military Cooperation: Past Events," U.S. Department of State Web Site; available at http://m.state.gov/mc38712.htm.

[170] Loek Essers, "Russian Cybercriminals Earned $4.5 Billion in 2011," *ComputerWorld* (24 April 2012); available at http://www.computerworld.com/s/article/9226498/Russian_cybercriminals_earned_4.5_billion_in_2011.

[171] "The G8 24/7 Network of Contact Points Protocol Statement," December 2007; available at www.oas.org/juridico/english/cyb_pry_G8_network.pdf.

[172] TASS, "Russia Calls for Cooperation in Combating Child Pornography," *Voice of Russia Radio* (1 June 2012); available at http://english.ruvr.ru/2012_06_01/76693555/. For example, in spite of its public statements, Russia is not one of the forty-nine countries that formed the Global Alliance Against Child Sexual Abuse Online in December 2012. See also United States Department of Justice. "Attorney General Eric Holder and High-Level Officials Launch Global Alliance against Child Sexual Abuse Online," Department of Justice Web Site (4 December 2012); available at www.justice.gov/opa/pr/2012/December/12-ag-1438.html.

[173] Ellen Barry, "After Boston Bombing, American Ties with Russia Improve," *New York Times* (29 April 2013).

ship and improve interaction by both sides in keeping with the countries' Mutual Legal Assistance Treaty.[174] Improved coordination should not be taken as a given in spite of the recent thaw, but a narrow window has opened for the U.S. to complement its usual efforts to press Russia on cybercrime in a way that could help address this critical organized crime issue.

Adopting Shared Public Key Infrastructure Standards. Public Key Infrastructure (PKI) is a technical concept that uses a "digital electronic signature" to verify the integrity of data and the identity of the sender during an exchange of electronic information. A 2008 report prepared for then-President-elect Obama warned, "Creating the ability to know reliably what person or device is sending a particular data stream in cyberspace must be part of an effective cybersecurity strategy."[175] PKI technology is an important means of providing that assurance. Its implementation in the U.S. DoD by means of Common Access Card (CAC) login, for example, resulted in a 50 percent drop in the frequency of cyber attacks the year after it was introduced.[176] The U.S. committed to working with other nations in its 2011 *National Strategy for Trusted Identities in Cyberspace*,[177] but it has proven hesitant to accept Russian overtures toward collaboration over fears of Russian attempts to control Internet content and limit its use by dissidents.[178] In spite of this, a technical working group should conduct a joint assessment of requirements and standards, with the short-term goal of developing common U.S. and Russian PKI standards in a manner that balances security requirements with civil liberties.[179] A bilateral agreement on such standards—particularly one that was technically compatible with other existing agreements—would be an important milestone toward a broader, multilateral consensus on electronic identity management.[180] Subsequent efforts could focus on creating structure and incentives for the U.S. and Russian private sectors to cooperate on future PKI standards and policy recommendations.[181] All of these measures would also help address U.S. concerns about cybercrime, Russian worries about "false flag" attacks, and shared problems in securing critical infrastructure from cyber threats.

[174] *Mutual Legal Assistance Treaty between the United States of America and the Russian Federation* (17 June 1999); available at www.state.gov/documents/organization/123676.pdf.

[175] Center for Strategic and International Studies, *Securing Cyberspace for the 44th Presidency. Report of the CSIS Commission on Cybersecurity for the 44th Presidency* (Washington, D.C.: Center for Strategic and International Studies, 2008), 62.

[176] Ibid.

[177] Office of the President of the United States, *National Strategy for Trusted Identities in Cyberspace* (Washington, D.C.: Government Printing Office, 2011), 4.

[178] John Markoff and Andrew E. Kramer, "U.S. and Russia Differ on a Treaty for Cyberspace," *New York Times* (28 June 2009).

[179] Gady and Austin, *Russia, the United States, and Cyber Diplomacy*, 9–12.

[180] See Combined Communications-Electronics Board, "PKI Cross-Certification Between CCEB Nations" (30 July 2007) as an example, outlining PKI standards for Australia, Canada, New Zealand, the United Kingdom, and the United States. Available at http://info.publicintelligence.net/CCEB-PKI.pdf.

[181] Gady and Austin, *Russia, the United States, and Cyber Diplomacy*, 11.

Reaching Consensus on International Law for Cyberspace. Because of the disagreement between the U.S. and the Russian Federation and their respective allies on the basic issue of the adequacy of existing international law in addressing cybersecurity issues, the development of a global consensus on these important subjects has been slow and uneven. Although Russia has long urged the development of a global treaty to regulate cyberspace, the lack of broad international support makes such an agreement extremely unlikely. Nevertheless, concurrence on norms of behavior in cyberspace is overdue and essential – and still achievable without a comprehensive international legal accord. Rather, a patchwork of bilateral or more limited multilateral agreements that share commonalities will, over time, generate agreement on the principles that are most broadly shared. While holding opposing views on many issues, the U.S. and Russia share similar perspectives on some important points. For example, a 2011 Russian document on military operations in cyberspace conceded that the international humanitarian law principles of discrimination, use of protective indicators, and prohibition on treachery apply in cyberspace.[182] While hardly earth-shattering, this concession does reveal some points of overlap in U.S. and Russian interests, and provides a point of departure for a program of engagement. This is an effort that the East-West Institute has already undertaken as a Track 2 diplomatic initiative to explore how to handle "humanitarian critical infrastructure" and how to apply the "distinctive Geneva emblem concept" (like the Red Cross or Red Crescent) in cyberspace.[183] Efforts like these should be encouraged and reinforced and, when sufficiently mature, moved into official diplomatic channels for codification – essentially adding one tile at a time to the mosaic of customary international law that will have to suffice in the absence of a comprehensive international treaty.

Conclusion

The relationships between the United States and Russia and NATO and Russia are difficult, messy affairs, with occasional highs punctuating long stretches of uncomfortable coexistence, periods of contentiousness, and intermittent unbridled acrimony. The policy issues that keep the two sides at loggerheads seems to continually refresh, with each resolved problem being replaced by another seemingly intractable dilemma almost immediately. Trust is in short supply in these relationships, along with a deficit in perceived mutual respect and equality from the Russian side that colors all interactions with the other side. In spite of these problems, Russia, NATO, and the U.S. share highly interdependent relationships politically, diplomatically, military, economically, and in many other important dimensions. In short, they need one another, particularly to address

[182] Ministry of Defense of the Russian Federation, "Conceptual Views Regarding the Activity of the Armed Forces of the Russian Federation in the Information Space."

[183] Karl Frederick Rauscher and Valery Yashchenko, eds., *Russia–U.S. Bilateral on Cyber Security: Critical Terminology Foundations* 1 (New York and Moscow: EastWest Institute and Moscow State University, April 2011), 7; available at www.ewi.info/system/files/reports/Russia-U%20S%20%20bilateral%20on%20terminology%20v76%20%282%29.pdf.

many of the key challenges in the current international environment, many of which demand regional or even global responses. One such issue is cybersecurity, where all three parties are among the leaders in terms of capability but where contradictory understandings of the nature of cyberspace and its uses have prevented them from banding together to tackle the many challenges posed by the cyber realm. Although progress will not be easy, U.S., NATO and Russian interests intersect in several key areas—technical capacity and standards development, threat intelligence sharing, interoperability enhancement, and consensus building on international law—that are fit for further exploration. By accepting limited and prudent risks in order to pursue this agenda, all sides stand to gain, with early advances on these subjects setting the conditions for further collaboration on cybersecurity and perhaps on a broader range of subjects as trust is generated and the habits of cooperation take hold.

Security Agencies and Parliamentary Committees of Inquiry in Germany: Transparency vs. Confidentiality

Sebastian von Münchow [*]

Introduction

"Good governance" is the political concept through which transitional and post-conflict states seek to be integrated into those parts of the international community that embrace the ideals of democracy and the rule of law and place a premium on the will of the people. One of the most decisive factors for the implementation of good governance is in how the security sector interacts with the state and contributes to the public welfare. In particular, the security sector should be subject to civilian oversight and control, make decisions that are comprehensible, and be held accountable for misconduct and unlawful actions.

This concept has led to a worldwide movement for security sector reform (SSR). As the global SSR agenda has been developed and implemented over the past decade, there has been increasing pressure to better integrate the security sector into the state in an effort to restrict the use of security forces as oppressive tools for power by a particular regime, clan, or individual. This is the most important task facing those countries that are embarking on SSR processes in an effort to align themselves more closely with the Euro-Atlantic security space, as the most crucial element in reforming a security sector is to build a nationally-owned and led vision of security that embraces modern-day standards of transparency.

In this light, several states in the Caucasus, Southern Europe, and the Middle East have launched reform initiatives to strengthen parliamentary control and governmental oversight over police services, the military, and intelligence services. There are numerous examples where previous security sectors of states within those and other regions have been involved in serious human rights abuses and have colluded in maintaining a corrupt or tyrannical regime. Considering this sometimes difficult background, it becomes even more obvious what a huge effort a reform seeking transparency in the secu-

[*] Dr. Sebastian von Münchow is a lecturer of security studies and international/European law at the George C. Marshall European Center for Security Studies. He studied law at the Free University of Berlin, the Université de Lausanne and the Christian-Albrechts-University Kiel. After receiving the Masters of Law, he took the Berlin bar exam and earned his doctorate in international relations from the University of Vienna on multilateral engagements in post conflict peace-building. Dr. von Münchow then worked for the field missions of the Organization for Security and Co-operation in Europe in Bosnia and Herzegovina, as well as in Kosovo. He has also served in the Police Assistance Mission of the European Union in Tirana. In Brussels, he joined the Office of the Special Coordinator of the Stability Pact for South Eastern Europe where he headed several initiatives to strengthen the home and justice sectors in the Balkans. After returning to Germany, Dr. von Münchow became government official and worked for several years in the Federal Chancellery.

rity sector actually entails. Visible indications of the implementation of good governance are vague at best with respect to both internal and external security, making them particularly difficult to identify. However, if parliamentary control and closer supervision by the ministries of the civilian government lead to the exposure of serious deficits within the power apparatus of the state—especially in the sensitive field of intelligence services—and succeed in drawing reasonable conclusions without reverting to historic behavioral patterns, then this would be counted as a strong indication of progress. The Federal Republic of Germany has spent decades reforming their security sector, and can serve as an example that other states might follow.

Over the last few decades the Federal Republic of Germany has developed a complex system of checks and balances to provide oversight within the security sector. Some of the checks and balances that have been put into place within the many layers of the security sector to ensure there is sufficient oversight are:

- Distinctions between the fields of responsibility for federal and state agencies
- An emphasis on the different aspects of oversight in the form of parliamentary control and executive supervision of the security sector
- A consistent judicial system, along with institutions such as the permanent Parliamentary Control Panel
- Investigations into and the publication by the media of misconduct and unlawful actions.

Similarly, other Western-oriented states have created diverse mechanisms for control and oversight of their security sectors, wherein the scope, means of intervention, and composition of responsible authorities vary. More often than not, the balancing act between the executive and legislative branches has led to the establishment of expert or parliamentary institutions dedicated to questions of budget, lawfulness of actions, and strategic alignment of the intelligence services.

Unique to Germany are the ad hoc parliamentary Committees of Inquiry (COI) at the federal level. In the past, these special-purpose committees focused on security issues and how German authorities dealt with them. Certain tensions naturally arose between the legislative and executive branches of the government. The parliamentary side invoked the general public's interest to clarify the respective circumstances and demanded that the inquiries be appropriately rigorous. For their part, the security agencies sometimes hesitated to disclose sensitive information. And this is exactly where the distinction from other models of oversight and control lies. In contrast to many other permanent oversight and control institutions, the members of a parliamentary COI in Germany enjoy largely unrestricted access to classified material, and benefit from the witnesses' duty to appear at the hearings, as well as from the possibility of public denunciation of any misconduct or illegal actions on the part of the security and intelligence services. The intensive investigative methods that are at the disposal of the members of the COI during an inquiry—which is always seeking a balance between the need for confidentiality and the right to inform the public—is what makes the German approach interesting for those states that are looking for models of how to exercise better control over their security sector, including the intelligence services.

By referring to specific cases, I wish to outline the nature of the German committees of inquiry. The task of balancing confidentiality and transparency will become obvious in the elaboration of legal matters and the presentation of the actual methods and practices utilized by the government. The article closes with considerations of whether the German COI can serve as a model for states in a transitional phase.

A Look at Previous COIs

Looking at the situation in Germany over the past twenty years, one can see that every legislative term has seen at least one incident in connection with foreign and security policy that led to an inquiry at the federal level that lasted several years and whose discussion elicited considerable emotion.[1] These committees were repeatedly under close scrutiny by the media, and some of them generated significant public outcry, leading to some ministers or senior administrators being disciplined or even resigning from their posts. The political parties involved in the inquiries position themselves according to a recurring pattern: while the opposition interprets the facts of a case as scandalous, the respective government coalition being scrutinized tries to comment on the proceedings as little as possible or appease their political opponents.

During the twelfth legislative term, the role of the former head of the Department for Commercial Coordination in former Eastern Germany, Alexander Schalck-Golodkowski, was subjected to inquiry.[2] Only one year later, during the thirteenth legislative term, from 1995–98, the Federal Intelligence Service (BND) had to justify its actions in connection with the so-called "plutonium scandal."[3] Foreign policy was at the center of

[1] This approach contrasts with investigations in the German federal states, which tend to concentrate on the use of public funds – usually in controversial large-scale construction projects. See, for example, Stuttgart 21, "Recommended Decision and Report of the Committee for Transport, Construction and Urban Development," BT-D print17/5172 (22 March 2011); and "Assessment Report of the Parliamentary Committee of Inquiry: Elbe Philharmonic Hall, Citizens of the Free and Hanseatic City of Hamburg," print 19/8400 (21 January 2011), 5.

[2] See the "Recommended Decision and Supplementary Report of the First Committee of Inquiry: Scrutiny of the role played by the 'Commercial Coordination' department and its head Alexander Schalck-Golodkowski in the SED leadership, state control and the economy of the GDR, and findings on who benefited or benefits to this day from the economic activities of this department," Bundestag print 12/8595 (2 November 1994), 39.

[3] See "Recommended Decision and Report of the First Committee of Inquiry: Findings on the Munich Plutonium Incident and issues related to this and other incidents, with a focus on the responsibility of the federal government and the personnel of federal agencies" ("Plutonium COI"), Bundestag print 13/10800 (28 May 2008), 45.

attention in the so-called "visa affair" during the fifteenth legislative term,[4] and the following term then saw what is probably the most substantial parliamentary inquiry to date into the work of German security agencies. The COI put several individual cases under scrutiny, such as those of Khaled El-Masri, Mohammed Zammar, and Murat Kurnaz, who were each temporarily apprehended overseas in connection with the U.S.-led war against terrorism, German activities in Baghdad during the third Gulf War, and the oversight and surveillance of journalists by the security sector under the pretenses of force protection and operation security.[5] During the seventeenth legislative term, the Defense Committee came together as a COI and questioned the legitimacy of a German air strike against two gas trucks in Kunduz, Afghanistan, in September 2009.[6] Starting in 2012, another committee was set up to investigate a neo-Nazi gang, the so-called "Zwickau Cell," whose crimes had gone undetected for years.[7]

In contrast to this are those security-related issues that were discussed in public but never made it to the COI level. In this context, the German Minister of Defense at the time and the Coordinator for Intelligence Services in the German Chancellery resigned from their posts in the early 1990s following discrepancies related to the export of weapons from the former East Germany.[8] Another case that was never investigated in a committee was that of a journalist whose private e-mail traffic had been unintentionally intercepted by the German intelligence service BND in 2008.[9] It was handled by the Par-

[4] See "Recommended Decision and Report of the Second Committee of Inquiry: Findings on whether members of the federal government or other government officials have in any way compromised or endangered the security of the Federal Republic of Germany or of other Schengen countries as of October 1998 when implementing immigration law through decrees, instructions or otherwise, in particular through the issuance of visa at German diplomatic missions, in particular in Moscow, Kiev, Tirana and Pristina" ("Visa COI"), Bundestag print 15/5975 (2 September 2005), 285.

[5] See "Recommended Decision and Report of the First COI: Open questions concerning incidents in relation to the war in Iraq and the fight against international terrorism" ("First COI of the Sixteenth Election Period"), Bundestag print 16/13400 (18 June 2009), 353–418.

[6] See "Recommended Decision and Report of the Defense Committee of the First COI: Inquiry into the command issued by the military leader of the provincial reconstruction team (PRT) in Kunduz/Afghanistan to carry out an air strike against two gas trucks on 3 and 4 September 2009, into the reconnaissance and information policy of the federal government, as well as into the compatibility of the chosen courses of action with national and multinational political, legal and military guidelines for the mission in Afghanistan" ("Kunduz COI"), Bundestag print 17/7400 (25 October 2011), 29, 169.

[7] See "Request to Set up a Committee of Inquiry," Bundestag print 17/8453 (24 January 2012).

[8] See "Reply by the Federal Government: Procurement of weapons from the East by the Federal Intelligence Service and transit shipment to friendly states," Bundestag print 12/2513 (30 April 1992).

[9] See "First COI of the Sixteenth Election Period," 474.

liamentary Control Panel, a permanent body that oversees the work of the intelligence services at the federal level.[10]

Preliminary Stages of a Committee

In the past, security policy issues that eventually became the subject of a parliamentary inquiry were usually not the focus of discussion within the political arena or the media until shortly before or after federal elections. The reason for this is, on the one hand, the uncertain outcomes of the election campaign itself and, on the other hand, the potential party coalitions of both the government and opposition that would take shape after the elections. The experience of how intensely the public follows this kind of inquiry may serve as an inspiration to any opposition party to find a topic with the potential to bind a government for years to come.

To mention only one example, in late 2005 and early 2006, the new federal government tried to thwart the creation of a COI by publishing a report aimed at countering the allegations in the media and the increasing number of critical questions regarding the war on terror in the regular Bundestag (the lower house of parliament) committees.[11] The attempt failed. In a scope probably unparalleled anywhere in the world, the security agencies had gathered material to rebut the criticism. But the opposition parties still had "open questions," and it was decided that a committee should be set up.[12] One conse-

[10] The Parliamentary Control Panel is responsible for the oversight of federal intelligence agencies. The federal government is obliged to inform the committee in detail about the activities of the intelligence services. Its consultations are subject to strict confidentiality and non-disclosure – see http://www.bundestag.de/bundestag/gremien/pkgr/index.jsp and Dietmar Peitsch and Christina Polzin, "Die parlamentarische Kontrolle der Nachrichtendienste" ["Parliamentary Control of the Intelligence Services"], *Neue Zeitschrift für Verwaltungsrecht* (2000): 387–93. It is worth mentioning that most states do not have any independent parliamentary oversight of their intelligence services, but merely oversight structures in the responsible ministries. See Hans Born, "Towards Effective Democratic Oversight of Intelligence Services: Lessons Learned from Comparing National Practices," *Connections* 3:4 (2004): 1-12. See also Jelle van Buuren, *Secret Truth: The EU Joint Situation Centre* (Amsterdam: Eurowatch, 2009).

[11] See Dana Priest, "CIA Holds Terror Suspects in Secret Prisons," *Washington Post* (2 November 2005); available at http://www.washingtonpost.com/wp-dyn/content/article/2005/11/01/AR2005110101644.html. The federal government presented a final report "On the incidents in relation to the war in Iraq and the fight against international terrorism" to the Parliamentary Control Panel on 20 February 2006. To further investigate any remaining issues, and to determine assessments and possible consequences, a committee of inquiry was set up according to Article 44 of the Basic Law.

[12] See "The Green Party, the Liberals and the Left Party Decide to Set up a COI to Inquire into the BND Scandal," *Der Spiegel* online (17 January 2006); available at www.spiegel.de/politik/deutschland/bundestag-gruene-fdp-und-linkspartei-beschliessen-untersuchungsausschuss-zur-bnd-affaere-a-395748.html. See Also "BND-Ausschuss," *Die Zeit online* (12 April 2006); available at www.zeit.de/online/2006/15/BND.

quence, among others, was that confidential information was made public even before the COI had begun its work.

Setting up a COI at the federal level usually means that dozens, if not hundreds, of employees of the affected government agencies as well as the parliament's administration are tied up for several years. Huge amounts of original and copied files are moved and a large number of witnesses are brought to Berlin for hearings, some of them from far-away regions.

The Setting-up of a COI and its Relevance in Terms of Constitutional Law

A motion to set up a COI in the Bundestag can be proposed by a quarter of the members of the parliament—the so-called "qualified minority"—in accordance with Article 44, Paragraph 1, Section 1 of Germany's Basic Law. This makes it clear that an inquiry into misconduct and illegal actions is almost always possible, and cannot be rejected by a majority vote in the Bundestag. Thus, the right to have an inquiry is one of the most significant democratic rights in Germany. Parliamentary COIs are enshrined in the Basic Law and are part of those legal provisions guaranteeing the minority the greatest power to pursue their political agendas within the coalition-opposition arrangement.[13]

The decision to set up a committee must be made in accordance with the Constitutional Law. This means that the ability to limit the scope of the inquiry by means of interpretation must be adequately defined.[14] The Bundestag determines how many and which of its members will be part of the committee. The number mirrors the size of the various party groups making up that particular legislature. As a rule, either seven or eleven deputies respectively will form the committee. The chairman of the committee is a member of the strongest faction, and his or her deputy a member of the second strongest faction.[15] Generally, the sessions take place during the sitting weeks of the parliament. Special sessions can be convened, but must be approved by the President of the Bundestag.[16]

If the facts of the matter align with the portfolio of the Ministry of Defense, the Defense Committee will be responsible to constitute itself as a COI.[17] This occurred during

[13] See Reinhard Bergmann in *Grundgesetz für die Bundesrepublik Deutschland–Taschenkommentar* [*Basic Law for the Federal Republic of Germany–Pocket Commentary*], 7th ed., ed. Karl-Heinz Seifert and Dieter Hömig (Berlin: Nomos, 2003), 369.

[14] The decision to set up a committee of inquiry becomes effective if the subject of the inquiry is adequately defined. See Constitutional Court of Saxony, 154-I-07 (29 August 2008), 29; Decisions made by the Federal Constitutional Court 124, 78 [117]; State Court of Hesse, Decisions by the Administrative Court 17, 1 [17]; 22, 136 [140]; State Constitutional Court of Saxony-Anhalt, Decisions by the State Constitutional Court 15, 353 [358].

[15] See Sections 4–7 of the Committee of Inquiry Act.

[16] See Section 8, Committee of Inquiry Act.

[17] See Section 34, Paragraph 4 of the Committee of Inquiry Act; according to Article 45(a), Paragraph 3 of the Basic Law, no committee of inquiry can be set up for defense issues, nor can the Defense Committee be given an inquiry mandate.

the seventeenth legislative term to investigate the events surrounding the air strike in Kunduz, Afghanistan, in September 2009.

The Rights of the COI and of the Executive Branch

The rights of the COI are stipulated in the German Bundestag's Committees of Inquiry Act with reference to sections of the Code of Criminal Procedure.[18] This means that the COI's procedure is similar to that in criminal proceedings, especially with regard to the legitimacy of material evidence and witness testimony. Yet the committee is not a court of law. In the end, it merely compiles a report that is submitted to the President of the parliament.[19]

The factions can make motions to hear evidence in the COI. Only one-fourth of the votes of the committee members are needed for this. The COI hardly ever rejects such a motion, as it would risk being accused of obstructing the parliament's (and therefore the public's) access to information. But it is possible according to the law. Inadmissibility can be claimed if the motion to hear evidence is improper—for example, if it is intended to delay proceedings—or asks to inquire into a topic that is not covered by the COI's mandate.[20]

The federal government, on the other hand, has an obligation to support the COI in its mission to clarify the facts. This obligation for cooperation follows the principle that governmental officials must act in accordance with their respective constitutional duties, a principle that all constitutional bodies must adhere to. On a day-to-day basis this means, for instance, that no documents can be withheld from the COI, even if sharing them would be politically inconvenient. Witnesses related to the executive branch must tell the truth before the committee even when it conflicts with their political and positional interests.

The federal government has the right to dispatch representatives from all departments affected by the mandate who, in accordance with Article 43, Paragraph 2 of the Basic Law, are entitled to attend and to speak at committee sessions. However, the representatives may not direct questions to the witnesses called by the committee. They normally appoint a person to represent the government's position. This appointed representative has the right to ask the chairperson if the questions asked by the members of

[18] According to Section 36 of the Committee of Inquiry Act, there is the possibility to appeal to an investigating judge at the Federal Court of Justice. This was done during the work of the committee of inquiry in the sixteenth legislative term, overruling objections by the opposition. See "First COI of the Sixteenth EP," 48.

[19] The work of a COI can, however, lead to criminal proceedings. Witnesses have to tell the truth. If not, they can be sued for making false statements while not under oath, cf. § 153 Criminal Code. See also "Plutonium COI," 25.

[20] See Sections 10 and 17 of the Committee of Inquiry Act; and Bergmann in *Grundgesetz für die Bundesrepublik Deutschland–Taschenkommentar*, ed. Karl-Heinz Seifert and Dieter Hömig, Art. 44, Para. 2 (1), margin no. 6. Requests to present evidence make it possible to determine at an early stage which kind of evidence the deputies plan to use with regard to a subject.

the Bundestag perhaps go beyond the scope of the inquiry, or exceed or violate the right to take evidence. His function is similar to that of an authorized proxy at court.

Mandate for a COI

Any conceivable mandate for a COI basically follows the same pattern:

- Who did what, when, how, with whom, with what, and why?
- Was this lawful and/or politically appropriate?
- Which internal and/or political decision makers knew about it and bear responsibility?
- What are the lessons learned?

The last question is relevant only for the representatives of the Bundestag who can make suggestions for future action in their final report. However, the preceding questions are necessary for the legislative body to obtain the relevant information from the executive agencies. Generally, the mandate for a COI can be interpreted verbatim. The mandate dictates which facts will need to be investigated and where the political debates can be expected to run parallel to the inquiry.[21] The time period to be investigated begins at the initial point in time when the circumstances of interest took place. The end point is the day when the COI was set up. Currently pending actions may not be challenged, as this would undermine the prohibition of collateral control.[22]

The upper echelons of the departments involved in the COI make the fundamental decision of whether a mandate is to be interpreted in a broad or a narrow fashion. In the end, it is their decision whether to allow for greater transparency. A broad interpretation will lead to the presentation of a large number of files, and will require the witnesses to answer a wide range of questions. On the other hand, the consequences of a narrow interpretation might mean that only a small number of files will be considered relevant, and that witnesses may only be asked to answer narrowly defined factual questions.[23]

[21] In this context, certain phrases and terms may seem somewhat vague and create uncertainty. Therefore it is recommended to consult the decision recommendations, the minutes of the plenary debate, and/or statements made by individual deputies. See *Decisions by the Federal Constitutional Court* 124, 78 [118 f.]

[22] See *Decisions by the Bavarian Constitutional Court* 38, 165 [177]; Böckenförde, *Parliamentary Committees of Inquiry and Local Autonomy*, 1 f.; Achterberg/Schulte *Kommentar zum Grundgesetz* [*Commentary on the German Basic Law*], Vol. 2, 4th ed., ed. Hermann von Mangoldt, Friedrich Klein, and Christian Starck (Munich: Vahlen, 2000), Art. 44, margin no. 61.

[23] These basic guidelines may, however, be open to interpretation for practical purposes. While during the "First COI of the Sixteenth EP" Parliament was told quite clearly that, due to the nature of the cause, the government could only grant a limited degree of transparency, it received full, unconditional, and generous support during the investigations of the Kunduz committee.

Evidence

Orders from the committee to obtain evidence must be adequately defined and must serve the aim of gathering information. However, it is acceptable for the order to be vague to a certain degree. It is generally assumed that a line is crossed if the evidence orders resemble "a shot in the dark." It is important for the institutions of the executive branch that these orders use evidence that supports the mission of the COI. This means that these orders are like stencils that, if superimposed on the COI's mission, outline specific aspects for which they demand material evidence or witness testimony.

For example, consider an evidence order the COI submits at the beginning of its work, or whenever it calls a new case complex. When the committee members pursue a line of questioning concerning "who at what point in time, knew what, from whom, about available intelligence, motives, execution, and the consequences of the air strike," the corresponding order will usually request all files, documents, correspondence, etc., available from all agencies that are potentially involved. This simple example serves to demonstrate that all affected parts of the security sector, if possible, will try to gather all relevant documents and records available and connected to the COI's mission to bring before the parliament for clarification.[24]

But the key question is what is considered relevant, and therefore requires the authorities to bring the material before the parliament? This differentiation is vital not only in a legal, but also in a practical sense. Information that is not relevant is not part of the inquiry, and therefore need not be presented to the committee. It is illegal for parliament to conduct an inquiry that is too generalized. For example, it would have meant an abuse of authority if in the context of the investigation into the Kunduz air strike the committee had asked the Ministry of Defense and the German Armed Forces to turn over all documents ever produced regarding Afghanistan.

The question of who determines what information is relevant to a COI's mission was a contested constitutional issue during the sixteenth legislative term, and was brought before the Constitutional Court.[25] The Federal Constitutional Court ruled in July 2009 that the federal government's interpretation of relevance had violated the rights of the COI. The Constitutional Court did not grant the executive branch the discretion to decide which documents contain relevant information for the Bundestag and which ones do not. However, due to the realities of actual possession of the information, the executive branch continued to assume a *de facto* right of interpretation. It does so in light of the Bundestag's duty to clearly define the mandate of the COI. In the end, an unspoken compromise seemed to be in the best interest of both sides. In most cases, this is the obvious solution. For example, it cannot be beneficial to the inquiry to request information

[24] Things tend to get more complicated when the committee makes the decision to obtain evidence during the course of the investigation. It may happen that witnesses make statements about lines of action that had not been considered relevant before, or had simply been unknown. Usually the committee is interested in such surprise twists, which makes it necessary to request evidence that may lead to new findings.

[25] *Decisions by the Federal Constitutional Court* 124, 78 [118 f.]

on all activities in the Balkans if the only relevant aspect is the question of who knew what and when about the apprehension of a suspected terrorist in Bosnia-Herzegovina.

The Constitutional Court did not answer the question of whether the COI may request complete insight into existing files. After all, committee members theoretically know the file numbers from the documents that have been brought before them, but none has ever requested a complete file. One possible explanation might be that the members of the Bundestag are concerned that they will be overwhelmed by files and documents. The service provided by the government agencies to pre-select the relevant files seems more productive. Insisting on having full insight into all the events would indeed be less useful, as this would lead to the authorities being obliged to print out all press releases referring to the discussed topic. The number of files would increase dramatically.

But yet again, the decision of the Constitutional Court strengthened the parliament's interest in the disclosure of relevant files. It also ruled that it was not within the scope of the executive's authority to make the sole determination for or against transparency where sensitive information is concerned.

The Executive's Right to Withhold Documents

The question of whether there is evidence that can be withheld from the committee on legal grounds is another contributing factor to the tension in the effort to find a balance between disclosing and withholding information. The limits on the right to obtain evidence were also controversially discussed during the sixteenth legislative term. This played a role during the aforementioned case ruled on by the Federal Constitutional Court. On several previous occasions, the Constitutional Courts had determined the circumstances under which a government may refer to its right to withhold files from a parliamentary investigation. But for the complex inquiries of the committee during the sixteenth legislative term, only vague guidelines had been established by previous court decisions. The opposition seized the opportunity and used some rejected files, calling upon the Federal Constitutional Court to make a ruling on the scope of the parliament's right to conduct inquiries with regard to the limitations of the right to evidence.[26] They also attacked the narrow limitations imposed on witnesses who have been authorized to testify by the government's agencies. This was another occasion where the Constitutional Court strengthened the Bundestag's right to acquire information at the expense of the federal government's interests. On the other hand, the Constitutional Court also determined that the limitations on parliament's rights referred to by the federal government were not unlawful *per se*.

As a consequence, the government side rephrased their permissions to testify and the requirements for substantiation in order to comply with the court's ruling. Transparency was made paramount in those cases in which the committee would be denied access to documents. However, access to parts of or whole documents can be denied to parliament for the following reasons: for *Staatswohl* (national interest); the core areas of executive

[26] *Decisions by the Federal Constitutional Court* 67, 100 [142]; 76, 363 [387]; 77, 1 [46 f.] and "First COI of the Sixteenth EP," 48, 419, 478.

responsibility; basic civil and human rights; and the lack of original ownership over a piece of shared information.[27]

The Constitutional Court did not question the refusal to share evidence for reasons of the national interest *per se*, but they also chose not to provide any further clarification either.[28] It is assumed in this context that evidence could be kept from the committee—and thus eventually from the public—if it would reveal facts that could threaten the national interest or the vital interests of one of the sixteen federal states. That kind of threat is to be assumed if the publication of the documents would affect the continued existence or functioning of the state, threaten its internal or external security, or result in massive disturbances of public security and order. However, the court explained that this kind of threat could not be assumed if the publication would merely inconvenience the government. Furthermore, it pointed out that *Staatswohl* is entrusted in equal parts to the government and the Bundestag, and that the protection of sensitive information could be achieved through classification.[29] This reasoning held that the Bundestag, too, must respect the security, protection, and handling of information according to its classification. However, the ruling of July 2009 did not take into account the many press reports that were based on leaked documents.

However, withholding information to protect the national interest will remain the exception to the rule. In those cases, the government must carefully weigh the pros and cons of withholding evidence, and must carefully explain the decision in writing. Over the last few years, subcategories of *Staatswohl* have also formed, causing the authorities to remain reluctant to release certain documents. This is mainly the case where the core areas of the executive's responsibility and the protection of diplomatic negotiation processes are concerned, and in particular protection of the methods of the intelligence services. This point is of the utmost importance for the intelligence services due to their natural desire to keep their methods covert.

The core areas of the executive's responsibility include which initiatives, consultations, and actions are possible. As a rule, these are not accessible to a parliamentary COI.[30] Generally, the government should not be under constant supervision, and its members should be able to openly prepare and make decisions without the opposition's interference. This protection has been guaranteed by the assumption of an inaccessible "arcane sphere" of executive responsibility. This particularly refers to cabinet discussions and the preparation of cabinet and department decisions. There was no question of

[27] See "First COI of the Sixteenth EP," 24: "Number of files presented."

[28] *Decisions by the Federal Constitutional Court* 67, 100 [134] and *Decisions by the Federal Constitutional Court* 124, 78 [123].

[29] The Federal Constitutional Court had previously argued that it was admissible to apply the guidelines for classification to private secrets as well. See *Decisions by the Federal Constitutional Court* 67, 100 [135] and § 1, Rules of Procedure of the Bundestag.

[30] *Decisions by the Federal Constitutional Court* 67, 100 [133 f., 139 f.]; 110, 199 [214]; 124, 78 [120]; cf.: Volker Busse, "Der Kernbereich exekutiver Eigenverantwortung im Spannungsfeld der staatlichen Gewalten" ["The Core of Executive Autonomy among Conflicting Priorities of State Powers"], in *Die öffentliche Verwaltung* 42 (1989): 45.

the legitimacy of these assumptions; there were discussions, however, about what kind of evidence might fall into that category. Considering the clarifications by the Constitutional Court and the experience from previous committees, it is safe to say that the core area protects evidence that shows proximity to decision making and to issues that have not yet been resolved.[31] But determining exactly how to make these kinds of classification is difficult. As a general rule, it is to be assumed that a dossier is closed as soon as the government's decision-making process has reached maturity or the internal opinion making is finalized and results are ready to be released for external view. While it is possible, for example, to view the existence of a formal closing directive as the closure of a dossier, uncertainties in other fields remain. Many individual dossiers in connection with the global war on terror, for example, will not be closed in the foreseeable future. In this respect, the executive could persist in its viewpoint that parliament's interest in an investigation affects current dossiers. As a matter of fact, the following question would need to be answered in this respect: Would the disclosure affect the executive's decision making with regard to its current and future functionality as well as its discretion? In some cases, does the interest in maintaining confidentiality outweigh parliament's interest in investigating? Positive answers in both cases would have to be thoroughly justified. Parliament's interest in the investigation usually has more weight in scenarios where obvious breaches of the law are to be investigated. It is precisely in cases related to issues of foreign and security policy that the parliament will be able to refer to this reasoning.

The Constitutional Court ruled that withholding materials produced in preparation for Bundestag sessions or talks with representatives of foreign states was not permissible.[32] They criticized the government's letters of rejection for not being concrete enough, and held that a weighing of interests had not taken place. Hence, the Constitutional Court once again ruled in favor of transparency over the executive's arguments for discretion.

Third, the government referred to possible violations of fundamental civil and human rights that may be the consequence of a complete and open submission practice for files.[33] In particular, this applies to the fundamental rights to life and limb of intelligence

[31] This is applicable to the minutes of the federal cabinet, to cabinet notations, and submissions to facilitate the decision-making process, as long as no political decision has been made on the current dossier. See *Decisions by the Federal Constitutional Court* 124, 78 [122 f., 129 f.]

[32] See *Decisions by the Federal Constitutional Court* 124, 78 [170 ff.] on the "First COI of the Sixteenth EP."

[33] In the security services, this right to request the taking of evidence may be connected to the basic right to life and bodily integrity, to general personal rights, and to the right to informational self-determination. See *Decisions by the Federal Constitutional Court* 67,100 [144]. See also Dieter Hömig, in *Grundgesetz für die Bundesrepublik Deutschland–Taschenkommentar*, 7th ed., ed. Karl-Heinz Seifert and Dieter Hömig, Art. 10, Para. 1, margin no. 1a.

sources.[34] It is argued that, following a revelation, the source could face severe punishment or long prison sentences in many states. In this case, too, the result was that parliament's interest in obtaining information must be weighed against a violation of fundamental rights. In cases when the COI is denied access to information on such grounds, the government must produce substantial justification in a written statement as to the reasons why.[35]

The final, if contested, reason to withhold evidence is the lack of the right of disposal over a written piece of information. This concerns messages that German intelligence services receive from foreign services on the express condition that they must not be disclosed to a third party.[36] Enforcing this particular legal bar to obtaining evidence is of the utmost importance to all federal and state services, irrespective of the classification level. This would concern all the information received with the explicit statement or implicit assumption that it will be circulated only with the permission of the originator.[37] There has been a view that the prohibition against passing on this kind of information would nominally fall under the *Staatswohl* bar. It could be argued that the protection of the so-called "third party rule" ultimately serves the national interest, as the breach of this rule would mean becoming less trustworthy in the eyes of the nation's allies. As a consequence, Germany's international partners would cease to share sensitive information with Germany. This would, in turn, dramatically impair Germany's ability to combat terrorism, for example.[38]

[34] See Hömig, in *Grundgesetz für die Bundesrepublik Deutschland–Taschenkommentar*, 7th ed., ed. Karl-Heinz Seifert and Dieter Hömig, Art. 10, Para. 2, margin no. 5 f.

[35] See *Decisions by the Federal Constitutional Court* 124, 78 [123 f.], and *Decisions by the Federal Constitutional Court* 67, 100 [142]. Another matter that needs checking is whether the protection of basic rights can be guaranteed by a categorization according to the General Administrative Provision of the Federal Ministry of the Interior for the physical and organizational protection of classified documents of 31 March 2006.

[36] The right to informational self-determination may only be restricted if this is in the interest of the general public and in strict adherence to the principle of proportionality. The restriction may go no further than necessary for the protection of public interests; see *Decisions by the Federal Constitutional Court* 124, 78 [125].

[37] Information that has been obtained from a third member state or a third country can only be exchanged between the law enforcement authorities of two member states with the consent of that third state. See http://europa.eu/legislation_summaries/justice_freedom_security/police_customs_cooperation/l14581_en.html.

[38] The authorization to pass on this type of information has to be specifically requested. In most cases such requests remain unanswered. However, it has happened that partners have either explicitly released the information or maintained the information ban. See Jan Hecker, "Anmerkung zum BVerfG-Beschluss vom 17.06.2009" ["Comment on the Decision of the Federal Constitutional Court of 17 June 2009"], *Deutsches Verwaltungsblatt* 19 (2009): 1239 ff. See also Decisions by the Federal Constitutional Court 124, 78 [123 f.]. It is also conceivable that lacking power of disposal cannot be categorized as sufficient reason to withhold information. If the authorities cannot dispose freely of the information, they are not open for inspection by the parliament.

The above proves once again that the Constitutional Court imposes severe restrictions on the government's ability to withhold information for alleged security reasons. However, in the reality of a COI's work, it is to be considered normal that uncertainties regarding the relevance and the limits of the right to take evidence arise and often remain unresolved for several months. A de-escalation can be achieved with the help, for example, of the so-called "chairperson procedure," or the transmission of documents without acknowledging any legal obligation, or the informal discussion of disputed passages.[39]

Compilation of the Files

On the one hand, the federal government is obliged to provide evidence requested by a COI as quickly as possible, in a comprehensive fashion. On the other hand, government agencies need a certain amount of time to compile the extensive files containing the documents that are needed to come to a decision. As mentioned above, the files that are to be made available to a COI include all the documents to be found in the official files concerning the dossiers affected by the evidence order.[40] These can include notes, reports to the leadership, e-mails, letters, press releases with comments, reports, expert reports, etc. Contrary to what outsiders might expect, this means that there are no pre-existing sets of ring binders that only need to be pulled off the shelf and submitted to the Bundestag. Compiling these binders manually might appear trivial at first. However, it is this procedure that explains the immense expenditure of personnel and time. As the whole process of adding dividers, explanatory sheets, pagination, and writing comments regarding classification and reasons for removal is performed by hand, one might imagine the kind of complications to be expected during the process of compiling multi-volume binder sets.

[39] In a chairperson procedure, where only the chairperson and the chairperson's deputy have full access to classified material, a small group of deputies may be offered the opportunity to read controversial passages and check whether there is sufficient reason for holding back information. However, the Constitutional Court does not accept this procedure as an alternative to the detailed and substantiated assessment of the pros and cons in cases of the above mentioned bans on the taking of evidence. See *Decisions by the Federal Constitutional Court* 67, 100 [138f.]; 77, 1 [56]. Another de-escalation mechanism is the *ex gratia* consignment of documents. It is also used for the hearing of witnesses if it remains unclear whether remarks on facts and circumstances are within or beyond the scope of the inquiry. Of course, the federal government may volunteer evidence not considered relevant or subject to the taking of evidence. However, if such a procedure becomes a matter of routine, it may have a prejudicial effect.

[40] A "file" is defined as a collection of documents relating to the same matter which is treated and quoted as a whole, and usually carries a file number. The idea is to have all existing written information on the matter in question available at any time. This meets the written form requirement (documentary character), which is based not only on the existence but also on the availability of documents. A file register ensures the traceability of files.

This laborious process, along with the need to consult with other affected agencies regarding the content of the files, adds to the time delay. Basically, the departmental principle applies: the different departments compile their respective collections of documents on their own authority. Coordination is required in cases where there has been a previous exchange regarding the facts of the case. Then, hundreds of letters and reply letters, duplicates, and copies must be checked for congruence. There must also be congruence with respect to redacted passages in texts, classification, statements of reasons regarding claims to retain evidence, corresponding documents, and which documents are to be submitted and which ones are not. This might appear rather trivial at first sight, and yet this too is an active effort to get to the bottom of the matter at hand.[41]

One has to bear in mind that the respective departments often consider a multitude of files to be relevant to the facts of the matter. One can imagine the amount of man-hours needed when three or four different ministries and subordinate agencies each wish to align hundreds of pages with the files of the other departments. The past has shown that usually some documents end up being discussed for a rather long time, and often are the cause of significant dispute. In other words, the separate departments connected to the inquiry cannot provide congruent sets of files by simply "having a quick look" into the archives.

So far, there have never been any complaints about differences in style, structure, formatting, etc., between documents. This is not surprising, considering that the documents are studied by people who have never concerned themselves in depth with the events. Ultimately, full and complete congruence between all the different sets of files will never be achieved. The sheer volume of documents and files can easily amount to more than five hundred file binders. A complete alignment of the amorphous contents of files can hardly be achieved. It is difficult to imagine that a ministerial staff member will be able to remember after several months which passages had been blacked out in a document from another department. And this cannot be achieved in a parliamentary environment, either. In addition to that, the administrative practices of the federal govern-

[41] See "Committee Finds that Chaos Reigns in the Security Services," at www.bundestag.de/dokumente/textarchiv/2013/42632406_kw05_pa_2ua_nsu/index.html; "Request for Setting up a COI," Bundestag print 17/8453 (24 January 2012); "Interim Report of the COI 5/1: Possible misconduct of law enforcement and security services of the state of Thuringia, including the responsible ministries and their political leadership, as well as persons cooperating with security services (human sources) in the context of activities of right wing extremist structures, particularly the *National Socialist Underground (NSU)* and *Protection of the Thuringian Homeland (THS)* and their members, as well as possible mistakes made by the Thuringia Security Services and Law Enforcement in the investigation and prosecution of crimes committed by the NSU and affiliated networks." This became apparent when the COI was taking the evidence with regard to the murders committed by the terrorist group National Socialist Underground, the so-called "Zwickau Cell." Looking into the misconduct of several authorities was one of the committee's tasks, as well as getting an overview of the records as they stood at the time. Thüringer Landtag, print 5/5810; see also "We Literally Know Nothing, *Süddeutsche Zeitung* (14 September 2012); available at http://www.sueddeutsche.de/politik/pannen-bei-nsu-ermittlungen-wir-wissen-buchstaeblich-nichts-1.1467718.

ment and its departments *per se* can hardly become the subject of an inquiry. But in order to fulfill the high standards it sets for its administrative work, the government should continue to strive to avoid differences in the records if at all possible.

Testifying as a Witness in the Committee Sessions

Witness testimony is the second important pillar when inquiring about the facts of a matter. Generally, the COI requests the nomination of witnesses that are to be heard regarding a subject of inquiry via an evidence order. In this context, the security agencies must make sure that those employees are nominated who made relevant observations within the scope of their duties. Otherwise, almost all of the employees would have to be listed, as the debated events are normally known through the media.

According to Section 23 of the Committees of Inquiry Act, in connection with Section 54 of the Code of Criminal Procedure (CoCP), office-holders—that is, every civil servant employed within the German security sector—require permission to give evidence, the scope of which has been disputed before the Constitutional Court. Whereas in the past the permissions to give evidence had been rather narrowly defined, their wording became more abstract from July 2009 on in order to ensure the executive branch's openness with regard to the interest in transparency.[42] Foreign office holders, as a rule, receive permission to give evidence from their agency, too. So far, most efforts of committees of inquiry to receive permission to hear employees of U.S. agencies in particular have failed. Without going into further detail, the U.S. government has made it clear that it is also not possible to hear former employees as witnesses before the Bundestag.[43] Persons who have gained knowledge of facts relevant to the case in a different fashion are naturally under no compulsion to give testimony.

From the media's point of view, the testimony of witnesses is the most interesting part of evidence gathering. Bundestag members seize the opportunity to articulate their position in front of the cameras directly before or after the witnesses' testimony. With a two-thirds majority vote and the consent of the witnesses, there is the possibility to broadcast the sessions live on television.[44]

The chairperson opens the hearing of witnesses, and informs the witnesses of their rights and duties.[45] The time allotted to committee members for speaking or asking questions depends on the size of their faction in parliament. Members of the governing coa-

[42] Now witnesses need to quote substantive reasons to explain why in such a case the right to request evidence is limited. For legal experts, that may not be a problem, but it is asking a lot from those who are not familiar with constitutional discourse.

[43] See "Kunduz COI," 22: "Hearing of foreign witnesses."

[44] See Art. 44, Para. 1 of the Basic Law: "All taking of evidence is public." The Committees of Inquiry Act states that all audio and visual recording is prohibited and that, as a rule, broadcasting is not permitted either. Exceptions, however, are possible, if a two-thirds majority of the members present as well as the person or persons to be heard or to be questioned have agreed. See Decision by the 2nd COI ("Visa CoI"), Bundestag print 15/5975 (2 September 2005), 41: "Permission for sound and video recording and film footage."

[45] See § 20, Para. 2, Committees of Inquiry Act.

lition and the opposition take turns questioning the witnesses. This rotation technique is called "Berlin Hour."[46] It can be repeated as often as deemed necessary. At the end, the members get the opportunity to ask questions in an open forum.

When witnesses are summoned plays an important and often disputed role in committees of inquiry. In general, the committee tries to follow a certain dramaturgy, i.e. at first, lower-ranking office-holders and other witnesses are heard, with the committee climbing the ladder from department heads up to deputy ministers.[47] From the media's point of view, the committee hearings culminate with the testimony of the affected ministers, who must justify the actions (or failure to act) of the government regarding the respective matters of inquiry.[48]

The sessions always start out as public sessions, unless they are closed to the public from the outset. This is often the case when employees of the intelligence services are heard.[49] The exclusion of the public is determined in accordance with Section 14, Para. 1 and 3, and Section 15, Para. 1 and 3 of the COI Act. The reasons stated there do not allow for any discretion.[50] The classification of the session corresponds to the subject

[46] A Berlin Hour is the speaking time in plenary sessions or committees based on the number of seats in Parliament. The current Berlin Hour is sixty minutes, with twenty-three minutes allocated to the SPD and CDU/CSU respectively, nine minutes to the Liberals, and seven minutes each to the Green Party and the Left Party. In case of an overrun, the speaker is admonished by the chairman and then asked to stop. See Hermann Schreiner, "Die Berliner Stunde—Funktionsweise und Erfahrungen: Zur Redeordnung des Deutschen Bundestages" ["The Berlin Hour – How it works: The Rules for Speakers in the German Bundestag"], in *Zeitschrift für Parlamentsfragen* 36:6 (2005): 573–88.

[47] See "Kunduz COI," 18: "The sequence of hearings and recommendations for decisions" and report by the Second COI: "Investigation of the role of the Bundestag and, in particular, of the Federal Ministry of Finance in the proceedings concerning the Hypo Real Estate (Hypo-Real-Estate IC)," Bundestag print 16/14000 (18 September 2009), 35: "Sequence of Hearings."

[48] It sometimes happens that the members of the coalition and those of the opposition cannot agree on when to summon a certain witness. Usually, the summons is done according to the so-called zipper procedure: both sides make suggestions on who to hear, until the matter culminates in the hearing of a minister. There are other methods, too, such as calling a number of witnesses corresponding to the size of the faction or at a ratio of one for the coalition, one for the opposition.

[49] As a rule, only a limited number of visitors are interested in the proceedings. Media representatives, however, are usually present at the sessions when the hearing of witnesses promises to be interesting. Audio and video recordings are prohibited. They are, however, permitted right before a session, which usually results in pictures of ministers or high officials taking the witness stand.

[50] According to § 14 of the Committees of Inquiry Act, the public is excluded if personal issues of witnesses or third parties come up, and if the public discussion of these issues would harm interests worth protecting; endanger the life, health, or freedom of the individual witness or another person; or if the discussion of a business, trade, invention, or tax secret that is likely to be mentioned would harm interests worth protecting or would be detrimental to the federation or a state, particularly if the security of the federal republic or its relations to other states are concerned.

matter to be discussed. An ordinary resolution of the committee members is sufficient to bring this decision about. According to Section 12, Para. 3 of the COI Act, the statements made in closed hearings may not be made public by individual committee members; only the committee as a whole may make information public.[51] Yet sometimes in the wake of a meeting individual deputies will brief the media on the hearings. However, it is possible to protect classified materials and guarantee document security according to Sections 15 and 16 of the COI Act and to achieve the appropriate classification. Taking evidence that is classified as confidential or higher must then take place in another, secure, room.[52]

Sometimes a request is made that witness testimony and the COI's minutes be declassified so that statements can be entered into the record of the public hearings of witnesses.[53] It can also facilitate the discussion in the media regarding past misconduct. So far, the government has always complied after considering the parliamentary requests. As a consequence, the security agencies had to check all classified minutes and ensure that, after the redaction of sensitive passages, they were fit for publication. This often involves hundreds of pages and multiple departments. Thus, the coordination of proposals among the different security agencies as to which passages are to be redacted can be tedious.

As was explained above, the witness may refer to the limited scope of the permission to give evidence as a reason for declining to answer a question. The witness may also refuse to answer any questions of a speculative or hypothetical nature, and may adhere to his or her own observations and direct knowledge.[54] The COI members may, however, ask the witness about his or her assessment of events or persons, even if such assessment is abstract. If the witness does not wish to testify on a concrete question in front of the committee, or believes that the limits of the right to take evidence have been reached,

[51] Each member of the committee is free to inform the public about the consultations and the decision making in a session of evidence gathering which is "only" categorized as non-public. For the effective protection of secrets and classified materials that come from the domain of the government and are to be made public during a hearing of witnesses, additional protection is required. This type of physical and procedural protection is guaranteed by § 15 and § 16 of the Committees of Inquiry Act after the appropriate classification has been made.

[52] See § 14 of the Committees of Inquiry Act and § 9 of the Committees of Inquiry Act of the Berlin Chamber of Deputies.

[53] The COI decides whether witness testimonies are classified; see § 15, Paras. 1 and 2, in conjunction with § 14, Para. 3 of the Committees of Inquiry Act. The decision is usually based on the classification level of the relevant material. Documents published by the COI are solely subject to the Bundestag bylaws. Whether the minutes of hearings get declassified is first of all for the COI to decide. In such cases, the government has to make sure to get involved.

[54] The obligation to testify applies exclusively to facts, not to assessments, conclusions, legal issues, general impressions, assumptions, experience, etc. Questions relating to anything other than facts may get rejected as non-admissible.

the federal government's coordinator might be obliged to supply substantive justification for this.[55]

Leaks

Online, television, and print media closely follow the events surrounding the committee sessions. Why the security sector finds itself in the crosshairs of parliamentary inquiries again and again is a matter of speculation. Events featuring secret agents, war, undercover operations, the CIA, the hunt for terrorists, etc. appear to still hold a certain appeal for the media. This is comprehensible from the public's point of view, as these topics obviously guarantee a kind of drama that dry and complex processes of the financial and economic sectors will never be able to generate.[56] Besides that, they offer journalists plenty of opportunity to look into the questions of "who knew what and when did they know it" regarding political decision makers. Ultimately, this is another facet of both the public and the parliament's desire to inquire into cases of misconduct, corruption, and misappropriation of funds.[57]

During the last few COIs that dealt with issues concerning foreign and security policy, there were several publications in the press referring to documents that had been sent to the committee's secretariat only shortly before.[58] These documents were of all classification levels. How the few available copies of these documents came into the possession of the journalists was never established. In this context, the Bundestag declared that the access to classified documents, the circle of authorized persons, and the safe-keeping within the Secret Records Office is sufficiently regulated by the COI.[59]

Because the contents of the documents immediately became public, they could be easily quoted during the committee sessions. The government kept insisting that publication does not change the classification level, though this call often went unheeded in the public debate.[60] Witnesses were sometimes put in an awkward position. Quite often, they were confronted with newspaper articles publicly quoting classified documents

[55] When testifying before a COI, witnesses do not have to say anything that can be used against them. However, according to § 22 of the COI Act, the reasons for their refusal must be clarified. Therefore, facts and credibility are required – mere statements are not sufficient. See *Decisions by the Federal Constitutional Court* 124, 78 [131f.].

[56] See, for example, "Hypo Real Estate Committee"; "The Process of an Inquiry," 26 ff.

[57] Hans Born, "Towards Effective Democratic Oversight of Intelligence Services: Lessons Learned from Comparing National Practices, *Connections* 3:4 (2004): 11.

[58] See "First COI of the Sixteenth EP," 51 ff; "The Dilemma of Non-Disclosure."

[59] See "First COI of the Sixteenth EP," 51 ff: "Since it turned out to be impossible to guarantee effective protection of the documents made available by the federal government in spite of collective efforts, the head of the chancellery announced that the federal government intended to hand over material classified as confidential or with a higher classification level only on condition that the material be accessed exclusively at the Document Security Office of the German Bundestag."

[60] See § 9, Para. 1, Administrative Regulation of Classified Documents; § 3, Para. 2, Rules of Procedure of the Bundestag.

while the classification grade of the original information had not changed. Consequently, the authorities took into consideration that every classified document that is to be brought before the COI might become known to the press as well. Documents that were classified "confidential" or higher were henceforth exclusively sent to the Bundestag's Secret Records Office. This illustrates that on the one hand the leaks advanced the public debate to the disadvantage of the authorities' security interests, but that on the other hand the authorities reacted to these new circumstances by applying a more prudent process of submitting files and by taking administrative measures that at least slowed down the accessibility of sensitive documents.

Irrespective of the Bundestag Rules of Procedure, the question remains whether this kind of indiscretion falls within the purview of and is punishable under criminal law. The relevant legal regulations can be found in the German Criminal Code in Section 203, Para. 2 and Section 353 (b), Paras. 1 and 2. Where the employees of the security agencies as office-holders are concerned, unauthorized copying and distribution of documents constitutes a criminal offense. The situation is different for members of parliament and their staff. In any case, the President of the Bundestag would have to authorize the prosecution.

Prosecuting a journalist who accepted information from an office-holder is even more difficult. The point is that the primary offense—the disclosure of secret information—can only be committed by a person with access to classified information. It is a matter of dispute if a journalist can be accused of "successive aiding and abetting." No matter what, the journalist is under no obligation to name the source. Since the so-called "Cicero verdict" in February 2007, the source is protected under Article 5 of the Basic Law (which guarantees freedom of the press).[61]

So far, all of the lawsuits that have been filed were dismissed by the various prosecutors' offices. An outraged response from the executive branch would probably be met with incredulity by the public and media: illegal or inappropriate actions have been exposed, so how can the authorities possibly now investigate parliamentarians or journalists?

[61] In its verdict (*Decisions by the Federal Constitutional Court* 117, 244 [265 f.]), the Constitutional Court specified that the mere publication of an official secret by a journalist is not sufficient cause to justify a suspicion leading to search and seizure. Instead, specific facts are required, indicating that a person in a sensitive position was actually planning to publish the secret, which would then count as an offense susceptible to complicity. See "Draft Law on the Protection of the Freedom of the Press," Bundestag print 16/4539, 6 March 2007. See also "Criticizing Investigations Against Journalists," *Stern.de* (3 August 2007); available at www.stern.de/politik/deutschland/bnd-untersuchungsausschuss-kritik-an-ermittlungen-gegen-journalisten-594417.html. See also "Investigations Against Journalists for Breach of Secrecy," *faz.net* (2 August 2007); available at www.faz.net/aktuell/politik/inland/medien-ermittlungen-gegen-journalisten-wegen-geheimnisverrats-1459900.html.

Discontinuation of COIs

COIs are subject to discontinuation. This means that the investigation is terminated at the end of a legislative term, regardless of whether or not all the facts have been established or a final report has been completed.[62] A COI itself may encompass thousands of pages. It consists of four parts: procedures, fact-finding issues, assessments, and appendices. The secretariat submits the first draft to the parliamentary parties for comments. No official participation of the federal government is foreseen.

After adoption by the Bundestag, the report will be published. For security agencies, this means that ambiguous text passages that were not redacted prior to publication will be accessible to the public. It is possible that classified information will not be excluded from the draft. For reasons of transparency it is common procedure that many items of information are declassified before publication in accordance with Paragraph 33 of the COI Act. The Bundestag and the federal government endeavor to prevent the inadvertent release of classified material. Thus, classified documents are not referred to as such in the final report. Instead, the report indicates press releases that describe the indiscretions.

The parliamentary factions may provide commentary on the final report. Such statements sometimes run as long as several hundred pages.[63] Although issuing dissenting opinions is somewhat foreign to the German legal tradition, and is a recent borrowing from Anglo-Saxon legal practice, parliamentary statements seem to have become an established inquiry procedure. The factions may differ in their assessments, and sometimes even in their descriptions of facts and circumstances. As previously mentioned, there are no provisions for the executive branch to play a role in the production of or comment on a COI report.

Formally, a COI ends with the adoption of the final report by the Bundestag.[64] The chairman of the committee submits a copy to the President of the Bundestag. This may happen simultaneously to the presentation of the report to the press. The focus of public perception is not so much on the final report itself. Due to its sheer volume, it may not be read by a wide audience anyway. The report is perhaps primarily of interest to legal experts, humanities scholars, or future historians.

These procedures round out the work of the committee in the eyes of the public. Precarious issues are recalled, accusations are repeated or refuted, and emotional moments or situations are relived. For security and law enforcement agencies, COIs often mean

[62] See Rules of Procedure of the Bundestag, § 125; Wulf Damkowski, *Der parlamentarische Untersuchungsausschuss: Ein Handbuch für Wissenschaft und Praxis* [*The Parliamentary Investigation Committee: A Manual For Academics and Practitioners*] (Frankfurt: Campus Verlag, 1987), 31 ff.

[63] See “Kunduz-CoI,”; “Statements,” 413 ff.

[64] This usually happens during the last session of the Bundestag before the summer break—that is, approximately three years before the next elections. See, for example, ”First COI of the Sixteenth EP,” 18 June 2009; “Plutonium COI,” 28 May 1998; “Commercial Coordination,” 27 May1994; “Visa COI,” 2 September 2005.

that lessons will be drawn that may lead to new guidance in order to remedy shortcomings. For instance, some administrative procedures that seemed uncomplicated and straightforward in the 1980s and 1990s have been tightened considerably as a reaction to parliamentary COIs.

Serving as a Model?

The preceding analysis has demonstrated that there is tension between legislative requirements for transparency and executive constraints on providing information. This contentious situation exists at all levels – from trivial fact-finding to sophisticated legal interpretation by the Federal Constitutional Court. In June 2009, the Federal Constitutional Court weighed the "as much as possible" call for transparency against the "as much as necessary" call for the protection of information. In the end, priority was given to transparency over security concerns.

Reform-minded groups in states making the transition to democracy might perceive this decision as an encouragement to call for more transparency from their security sector as well. From an outsider's perspective, the depth of inquiry, the time and personnel involved, as well as the interrelated legal and political aspects might seem vastly complex. The German inquiry system, with its passion for detail, fits the Teutonic stereotype. However, the constant questioning and correcting of the work of the security agencies was fundamental in postwar Germany. Germany's parliamentary inquiry system is the result of a history that other states do not necessarily have to face with such intensity.

The legal complexity is understandable considering the requests bearing on foreign and security policy from various government and opposition party coalitions that the Federal Constitutional Court has had to deal with over time. In Germany, noncompliance with a Federal Constitutional Court decision is inconceivable. Therefore, the legislative and the executive branches are making efforts to integrate Federal Constitutional Court decisions into their administrative procedures.

It needs to be stated that a COI is not only a forum for discussing opposing legal opinions and interests. In Germany, it is also a forum for discussing fundamental political issues such as the fight against global terrorism, the out-of-area deployments of German soldiers, and Germany's position within alliances.

In transition and post-conflict states, one issue might be perceived with some skepticism: the disclosure of classified information. Sometimes operative details are published – information that in most states would be kept classified. Such transparency would probably not be supported in states where the intelligence services served as pillars of power over many decades. In SSR dialogues, foreign experts usually say that transparency is desired, but not to the extent that has been realized in a Central European context. Many states that are in the process of reforming their security sectors are often still struggling with unresolved internal and external conflicts. It is often emphasized that difficult security situations are not beneficial to transparent security agencies. In other words, the fragile security environment does not permit constant justification for actions taken by the security sector.

Transparency of security agencies is seen as something that economically prosperous states embedded in the geostrategic safety zone of the European Union can afford. Such statements need to be taken very seriously in discussions on SSR. Disentangling security structures from those of the legislative, executive, and judicial branches can be difficult, but it is important in order to find the proper checks and balances. Any serious efforts in this respect need to be honored. Reform initiatives need to take into account that each conflict presents its own conditions: conflicts in the Southern Caucasus are unresolved, conflict rhetoric in the Balkans is prevalent, and the Middle East has its own transitional dynamics. Well-meaning advice from a secure distance might be perceived by representatives of the executive branch and open-minded reformers as Western or Eurocentric arrogance.

At minimum, it is suggested that SSR projects in their beginning stages concentrate on establishing a functioning ministerial control system. Establishing permanent control organs with access to data may come next. Establishing parliamentary COIs comparable to German standards would eventually round out the reform process.

Independent of which forms of control and oversight over security agencies (including intelligence agencies) are established, it must be understood that parliamentary oversight entails a complex and detail-oriented inquiry system. It might serve as a matrix for identifying areas that are potentially deficient. In following this path, the executive and legislative branches will have to balance, permanently and in a multifaceted way, transparency and state protection. It might be convincing that, in the parliamentary control system, the executive branch has legal means and possibilities to avoid unnecessary disclosures. Committees should be seen as an opportunity to react to and correct the reasons for public criticism and to reveal controversial decision-making processes. If this approach leads to deficiencies in the security sector being identified and used to instigate institutional and personnel changes, then it should be considered a progressive step in Security Sector Reform and accordingly, Good Governance.

Energy Security: A Paradigm Shift

Velichka Milina [*]

Since the middle of the first decade of the twenty-first century, energy security has been among the highest priorities in the security strategies and policies of developed countries. The potential risks and threats related to energy security mainly grew out of two circumstances: the predicted upcoming production peak of hydrocarbon resources vital for the modern economy, and the security of their supplies. Two key factors in the past years, however, have dramatically changed the energy sector. The first factor is the global economic crisis of the 2010s, and the other is the strategic shock from the yield of non-conventional hydrocarbon resources. Today, energy security policy requires a paradigm shift and a new model of factors and conditions for its implementation. This article offers an analysis and assessment of the changes demanding a new paradigm of efficient energy security that is adequate to the changed realities of energy markets and global economic development.

The Old Paradigm [1]

The concept of energy security that dominated for almost forty years (following the energy crisis of the 1970s) was rooted in the relatively plentiful availability of and easy access to fossil fuels, while the main threat to global energy security was considered to be the discontinuation of energy supplies. Thus, the old paradigm could be briefly summarized as "stable and continuous supplies at affordable prices." The significance of this problem was suggested by the common statement of geopolitical strategists, investment bankers, geologists, and physicists on the foreseeable depletion of oil and natural gas, and by the "final countdown" that had started in the production of hydrocarbon resources at an acceptable "energy price."[2] This fact, as well as the severe competition for energy resources due to increasing demand and consumption in developed and emerging economies, shaped the context of energy policies.

This was a period when the major consumers of energy resources (the U.S., EU, China, and India) were highly dependent on the producing countries dominating the energy market from the Middle East and the Caspian region, Russia, etc. The basic principles of the energy market were energy nationalism, the active role of "transit" countries, and the domination of producers over consumers.

[*] Dr. Velichka Milina is Associate Professor of Political Science at the G.S. Rakovski National Defense Academy in Sofia, Bulgaria.

[1] See Velichka Milina, "Energy Security and Geopolitics," *Connections: The Quarterly Journal* 6:4 (Winter 2007): 27-46.

[2] The correlation between the energy necessary for the research and exploitation of energy resources and the energy contained in the sources. In case they are almost equal, the process of extraction of energy resources is meaningless.

Energy nationalism was the major principle that shaped the behavior of the key participants on the energy market, whether they were producing countries, transit countries, or heavy consumers of energy resources.[3] Energy nationalism created a reality where the behavior and decisions of energy markets and the supply of resources ultimately depended not on economic market factors but rather on the producers, whereas the energy market turned into an arena of interstate relations. Oil and natural gas were used as geopolitical weapons, while energy geopolitics and geoeconomics became the most essential part of global politics and the foreign policy of the key players on the energy market.

Energy (resource) nationalism is typical of exporting countries rich in hydrocarbon resources. As a rule, they follow the scenario of a phenomenon that experts diagnose as "the resource curse,"[4] or "the Dutch disease."[5] Its common feature is slow social and economic development of the country due to a lack of domestic economic stimuli, and because of local political elites who take advantage of the high export revenues to maintain closed political regimes. The main consequences are weak government institutions or authoritarian governments, restriction of civil and political liberties, lack of an independent judicial system and independent political parties, low economic effectiveness, and underdevelopment of the economy outside the extraction sector.

Negative internal economic and socio-political implications of the "resource curse" are the main reason for the big producers of resources to implement highly accentuated policies of energy nationalism. Thus, they enter into a cycle of mutual interdependence and repetition of the correlation between the internal effects of the "resource curse" and "resource nationalism":

1. High profits from energy resources allow autonomy of local elites and promote the "resource curse"
2. The political and economic effects of the "resource curse" increase oil dependency
3. The high degree of dependency increases the benefits of "resource nationalism"

[3] Due to the extreme importance for social development, in almost all countries the governments and national companies are responsible for maintaining reserves, conducting transportation, and ensuring access to energy resources. In general, oil and natural gas are government territories.

[4] Probably the only significant exemption is Norway, which managed to convert its income from resources into development. To a certain extent, this group includes also the U.S. and UK as countries rich in resources.

[5] This phenomenon was initially observed in the Netherlands when in the late 1950s the production boom of natural gas resulted in a series of negative economic effects. What is typical of countries with Dutch disease is that the value of their currency rises due to the fast flow of revenues from oil, gold, gas, diamonds or some other natural resources. As a result, the goods produced by the national economy become incompetitive and very cheap to export. The result is deindustrialization of the country.

4. High profits as a result of the policy of "resource nationalism" on the energy markets promote the "resource curse."[6]

These negative internal conditions resulting from the "resource curse" are the most frequently discussed phenomena in such states. At the same time, however, the effects of the "resource curse" have an impact on interstate relations in the energy sector (and others).

Studying the behavior of oil-rich countries, Thomas Friedman formulated what he called the "First Law of Petropolitics,"[7] which underlines the correlation between the increase of resources in oil and gas producing countries and their rising confidence in interstate relations and international policy. In the context of this law, it is important to take into account the effect of the interdependence between the "resource curse" and "resource nationalism" on globalized markets of energy resources and on international energy security.

The risks to energy security in importing countries caused by energy-producing countries could be the result of either intentional or unintentional actions.[8] First, the growth of unfavorable consequences from the "resource curse" increases the likelihood that producing states will intentionally act in the context of "resource nationalism." Second, the political and economic consequences of the "resource curse" could have undesirable negative effects on political stability in energy-producing countries and thus threaten energy security. The revolutions that took place during the so-called Arab Spring in North Africa and the Middle East have proved that the main destabilizing political and economic factors in the region result from the negative effects of the "resource curse," and they can not be considered as applying only to a specific country. Since it is impossible to predict what impact such instability may cause, or when it is most likely to occur, destabilizing trends in energy-rich countries that are victims of "resource curse" need constant attention. This is particularly true for the energy security of the European Union, which is surrounded by energy-rich countries, including Algeria, Libya, Egypt, Syria, Azerbaijan, Iran, Turkmenistan, Uzbekistan, Kazakhstan, and Russia. These are countries that are either major sources of energy supply for the EU or represent potential sources of diversification. It could be argued that many of them show

[6] See Ed Stoddard, "The Resource Curse – Resource Nationalism Nexus: Implications for Foreign Markets," *Journal of Energy Security* (21 November 2012); available at www.ensec.org/index.php?option=com_content&view=article&id=389:the-resource-curse-resource-nationalism-nexus-implications-for-foreign-markets&catid=130:issue-content&Itemid=405.

[7] "The First Law of Petropolitics posits the following: The price of oil and the pace of freedom always move in opposite directions in petrolist states. The higher the average global crude oil price rises, the more free speech, free press, free and fair elections, an independent judiciary, the rule of law, and independent political parties are eroded. And these negative trends are reinforced by the fact that the higher the price goes, the less petrolist leaders are sensitive to what the world thinks or says about them." Thomas Friedman, "The First Law of Petropolitics," *Foreign Policy* 154 (1 May 2006): 28–39; available at http://www.foreignpolicy.com/articles/2006/04/25/the_first_law_of_petropolitics.

[8] Stoddard, "The Resource Curse."

symptoms of resource curse and rentier state structures. Some—such as Russia, Turkmenistan, and Egypt, for example—sometimes explicitly manifest behaviors of resource nationalism. The United States also faces similar risks arising from its dependence on imported resources from the Middle East and Latin America when these countries share characteristics similar to the "resource curse" (e.g., Venezuela).

The negative effects of the "resource curse" are a factor not to be underestimated in the old but still functioning paradigm of energy security while developing strategies for the diversification and security of supply. Emerging new trends in the energy sector suggest some decrease in the role of the behavior of rich countries on energy security.

The New Context of Energy Security

In 2008–09, several key trends started to develop in the energy sector, triggered by the influence of two new, very strong factors: the global financial and economic crisis and the shale revolution in gas and oil production.

The Global Financial Crisis and the Energy Sector

The first factor to radically change the context of energy policies was the global economic crisis. Since 2008, experts have been analyzing its characteristics and causes. It has been defined as a financial crisis, an economic crisis, a crisis of democracy and governance, a crisis of public consumption and material culture as a whole, and as an environmental crisis that will ultimately lead to a global natural disaster. There have been disputes over the depth of the crisis, the patterns of its development, and its possible outcomes, but what unites analysts are the findings on the presence of the phenomena and processes of crisis and their global nature. From this perspective, it seems reasonable to argue that today we are experiencing a multidimensional global crisis, or the first systemic crisis of the global age.[9]

According to Nikolai Kondratiev's model, the depletion of the technological and organizational potential of the latest wave of growth determines the fact that crises of different origin that develop under normal conditions within their own sphere will start to interact and overlap.[10] The result is a kind of "resonance" of the crisis phenomena in different sectors: political, economic, social, energy, etc. Furthermore, any system, including the social one, has a limit of resistance, and such a resonance—especially if it is superimposed on adverse long-term trends and/or local short-term shocks—could knock a social system out of balance.

From 1900 to 2000, the dynamics of global development was determined by the then long-term hyperbolic growth in industry. Within this wave there were several phases

[9] See "Energy Sources and the Consequences of the Global Crisis of the 2010s," report at EnergyStrategy.ru (2012); available at http://www.energystrategy.ru/editions/krizis.htm (in Russian).

[10] On Kondratiev's waves and the contemporary economic crisis, see S. Y. Glazev, "Contemporary Theory of Wave Length in the Economic Development," available at www.group-global.org/storage_manage/download_file/20518 (in Russian).

separated by acute crises that led to a paradigm shift in development. These were the crises of the early 1930s, the crisis of the early 1970s, and the last one, at the end of the 2000s. For example, the crisis of the 1930s led to a sharp increase in the role of the state in the economy of the United States, Germany, Italy, and other industrialized nations. This process coincided with accelerated industrialization and a dramatic increase in the consumption of electricity for industry and oil as fuel.

The crisis of the 1970s led to the transition of the U.S. and Western Europe toward post-industrial development based on globalization, informatization, and liberalization of the socio-economic sphere. There was acceleration in the development of nuclear energy, and the demand for natural gas as an energy fuel grew.

In the late 2000s, the rate of economic and energy growth approached the peak rates seen in the 1950s and 1960s, with the highest rates being in developing countries. In fact, the most important feature of the pre-crisis growth period is the combination of post-industrial development in developed countries and rapid industrialization in developing countries (mainly China). During this period, however, the involvement of key developing countries in the global economy gradually exhausted the potential of globalization, informatization, and liberalization—i.e. the main elements of the third wave of growth—which became apparent during the global crisis of 2008–09. In the energy sector, this crisis coincided with the transition from "industrial" and "hydrocarbon" to "neo-industrial"[11] and "smart" energy, which includes a number of aspects: smart grids, energy efficiency (in the broad sense), renewable energy, new principles of organization of energy systems, and a shift of focus from the producer to the consumer.

These trends will be predominant in about twenty years. Up to 2030, all realistic scenarios for global energy production and consumption preserve the leading role of hydrocarbon fuels as sources of energy, although this does not preclude the shift to "neo-industrial" energy. According to expert estimates, in the energy markets this will take place through the convergence of the globalization and regionalization processes in the energy sector, as it is already happening in many industrial sectors.[12] Global domination of producers will be gradually replaced by domination of energy consumers, which could in the near future seriously change the current global situation in the energy sector.

[11] See A. I. Gromov, "New Driving Forces for the Development of Oil and Gas Complex," report at EnergyStrategy.ru (2012); available at http://www.energystrategy.ru/press-c/source/Gromov_NEA-4-12.pdf (in Russian).

[12] For details see the following publications in the Russian language: *World Energy: State, Problems, Prospects* (Moscow: Energy Publishing, 2007), www.energystrategy.ru/editions/mir_en.htm; V. V. Bushuev and A. M. Mastepanov, eds., *Global Energy and Sustainable Development: A White Paper* (Moscow: International Center for Sustainable Energy Development, 2009), www.energystrategy.ru/editions/white_book.htm; V.V. Bushuev and V.A. Kalamanov, eds., *White Paper: World Energy – 2050*, Second edition (Moscow: International Center for Sustainable Energy Development, 2013), www.isedc-u.com.

The Impact of the Shale Boom

The second factor that dramatically changed the energy markets was the quiet shale revolution in gas and oil production. Its effect on the prices of energy resources and geopolitics is still to be analyzed and assessed. What is going on, what are the parameters of the shale boom, and what are its geopolitical consequences?

During the first decade of the new century, expert analyses on energy security claimed that the peak in the production of hydrocarbon resources would occur within twenty years and then, unless an alternative source for the increasingly massive demand for fuel for industry and transport is found, mankind is doomed to economic apocalypse. No one had predicted the forthcoming (in 2008) occurrence of the "black swan"—the introduction of a new method for the production of unconventional (shale) gas at reasonable yield prices.[13] The essence of this method is horizontal drilling and hydraulic fracturing of the so-called shale rocks where oil and gas are not to be found in concentrated deposits, but are "spread" across the layers, stored in miniature cracks and porous pockets, and therefore can not be extracted with traditional drilling methods.

Today, as a result of the exploitation of these new technologies for the extraction of unconventional hydrocarbon resources, the United States since 2009 has been the world's biggest producer of natural gas, and according to the International Energy Agency, by 2020 they will replace Saudi Arabia as the largest oil producer.[14] A report by the U.S. Energy Information Administration from June 2013[15] points out that the shale oil reserves will increase the world deposits by 11 percent, and the shale gas formations will increase world natural gas deposits by 47 percent. As a share of all resources, shale oil constitutes 10 percent, while shale gas represents 32 percent. Here, however, we need to make a clarification. This data refers to technically recoverable but not necessarily economically effective resources. Technically recoverable resources represent oil and natural gas volumes that could be produced with current technology regardless of the production costs. Economically recoverable resources are those that could be profitably produced under current market conditions.

The economic recoverability of oil and gas resources depends on three factors: the costs of drilling and completing wells; the volume of oil or natural gas produced from an average well over its lifetime; and the prices received for oil and gas production. Recent experience with shale gas production in the United States and other countries shows that the assessment of economically recoverable resources could be significantly affected by

[13] "The Black Swan is a rare and unusual event that comes unexpectedly and is characterised by three features—it is unpredictable, it has huge impact and it could be explained by hindsight. Normal, routine and expected events are 'white swans.'" See Nassim Taleb, *The Black Swan: The Impact of the Highly Improbable in Life and on the Market* (New York: Random House, 2010).

[14] International Energy Agency, *World Energy Outlook 2012* (12 November 2012); available at http://www.worldenergyoutlook.org/publications/weo-2012/#d.en.26099.

[15] U.S. Energy Information Administration (EIA), "Technically Recoverable Shale Oil and Shale Gas Resources: An Assessment of 137 Shale Formations in 41 Countries Outside the United States" (13 June 2013); available at www.eia.gov/analysis/studies/worldshalegas/.

both geologic and non-geologic factors. Key positive non-geologic factors facilitating this kind of production in the United States and Canada that cannot be replicated elsewhere are the right of private ownership of underground deposits, which is a strong incentive for their development; the existence of many independent operators and supporting contractors with critical experience from various technological stages of production; and the availability of water resources to use in hydraulic fracturing.

For the time being, Poland presents the most disappointing illustration of the difference between technically and economically recoverable shale resources. The country has some of the most important proven reserves of technically recoverable shale gas in Europe. However, in May 2013, Canadian and U.S. companies refused to continue their studies and to engage in production in Poland due to the complex geology of shale fields and high population density in these regions – factors that increase the cost of production and make these deposits economically ineffective for mining. Thus, Poland had to give up its high expectations from the shale revolution that would make the country more independent of Russian energy supplies, and instead turned to more realistic projects to build a liquid gas terminal (2014) and a nuclear power plant (up to 2020).

After this clarification about a certain conditionality (in terms of actual production) in the stock levels of technically recoverable shale oil and gas, the lists released by the U.S. Energy Information Administration show the rankings of the top ten nations possessing these resources:

Table 1. Top 10 countries with technically recoverable shale oil resources.[16]

Rank	*Country*	*Shale oil (billion barrels)*
1	Russia	75
2	U.S.	58
3	China	32
4	Argentina	27
5	Libya	26
6	Australia	18
7	Venezuela	13
8	Mexico	13
9	Pakistan	9
10	Canada	9
	World Total	**345**

[16] Ibid.

Table 2. Top 10 countries with technically recoverable shale gas resources.[17]

Rank	*Country*	*Shale gas (trillion cubic feet)*
1	China	1,115
2	Argentina	802
3	Algeria	707
4	U.S.	665
5	Canada	573
6	Mexico	545
7	Australia	437
8	South Africa	390
9	Russia	285
10	Brazil	245
	World Total	**7,299**

The shale revolution, which to date is a fact only in the United States and Canada—the only place where economically significant amounts of unconventional energy resources are being produced—will have serious implications on the global energy market. Unconventionally produced natural gas has fundamentally changed the world market. Only five years ago the United States was expected to be a major importer of gas. Between 2000 and 2010, the country built infrastructure to reconvert to the gaseous state (regasification) over 100 billion cubic meters of imported liquefied natural gas (LNG) per year. In 2011, however, the United States imported just under 20 billion cubic meters of LNG.[18] Currently, efforts are being made to reconstruct unused regasification terminals in facilities for gas liquefaction in order to export LNG. The availability of large amounts of liquefied gas intended for the U.S. market has led to a significant fall in prices, with two main consequences: 1) Gazprom had to shorten the terms and lower the prices in its long-term contracts for supplies in European countries; 2) a number of these countries took steps to build terminals for liquefied gas as a policy to reduce their dependence on supplies through fixed grids.

Cheap natural gas is used in the U.S. to produce about 30 percent of the nation's electricity and to heat half of its households. The effect is that large amounts of coal, which had been used for this purpose, are being made available and appear on the world market at low prices. In Europe, this causes a distortion of the energy mix, and reduces the use of more expensive natural gas. In fact, the collapsed market of carbon emissions

[17] Ibid

[18] See http://e-vestnik.bg/14811.

does not impede the enhanced combustion of coal in Europe either, where gas stations (Belgium, Netherlands) are operating at a loss.[19]

The shale revolution in the U.S. has implications for global economic competition as well. For example, the price of natural gas for U.S. industry is one-fourth of the price in the EU, which harms the competitiveness of European companies.[20] The widening gap between the North American and European oil and gas markets highlights the competitive differences in crisis situations in exporting countries. The energy market in the U.S., unlike the EU, remained virtually untouched because of its growing autonomy from the political events in North Africa and the Middle East.

The most serious consequence of the shale gas revolution is the shift in the focus of the global gas market it is causing, from a market of producers to a market of consumers (the oil market is still dominated by producers). Several periods could be outlined in the producer-consumer relationship in the energy markets.[21]

The first one, starting with the discovery of oil in the late nineteenth century, was characterized by the dominance of (mostly Western) international oil companies in terms of energy resources and continued until 1970. The second period, which displayed greater control by the producing countries over their resources, was evidenced by the creation of OPEC in 1960 and the oil embargo of 1973. The third period began with the collapse of the Soviet Union, the spread of liberal values such as democracy and market economy, and the empowerment of liberal international institutions. Liberalization in the energy sector meant that energy was to a significant extent dependent on the logic of free markets. During the past ten years, however, the producing countries have been increasingly resorting to political considerations in their management of energy and have begun to apply the ideology of "energy nationalism." To these three we should add the fourth era, which has already started and is characterized by an excess of natural gas on the market and a focus on the user as the major figure.

Apparently, the contemporary global energy picture is going to change further. The peak of the international trade in energy resources, according to a number of evaluations, will occur around 2030. Today's dominant trend of resource globalization will be replaced by resource regionalization, while the fundamental focus is expected to be oriented towards domestic energy resources, including renewables. With resource regionalization, the share of technological and organizational globalization will grow. In this

[19] "Uncertainty Confused the European Energy Market," *Capital* (4 March 2013); available at http://www.capital.bg/politika_i_ikonomika/sviat/2013/03/04/2015507_nesigurnost_oburka_evropeiskiia_energien_pazar/?ref=rcmnd (in Bulgarian).

[20] European Commission President Jose Manuel Barroso, "Energy Challenges and Policy," European Commission Report to the European Council of 22 May 2013; available at http://ec.europa.eu/europe2020/pdf/energy2_en.pdf.

[21] See Kirsten Westphal, "Energy Policy between Multilateral Governance and Geopolitics: Whither Europe?", *Internationale Politik und Gesellschaft* 4 (2006): 47; cited in Raphael Metais, *Ensuring Energy Security in Europe: The EU between a Market-based and a Geopolitical Approach,* College of Europe, EU Diplomacy Paper 03/2013; available at http://aei.pitt.edu/42924/.

new context, serious changes will occur in energy policy and in the behavior of the main players on the energy market.

Major Players and the New Energy Market

Under the old paradigm of energy security, major players in the energy market competed mainly in the geoenergy sector, while energy resources were used as a "playing card" to achieve geopolitical dominance.[22] Today, the key players are the same, but some of them have already changed positions in the market. The new entrant into the ranks of the major actors is Canada. It has proven huge reserves of unconventional oil and gas and has long-term contracts for export (until 2019) of shale gas from British Columbia to East Asia.[23]

The United States

The United States is undoubtedly the new energy leader. They have owned this position since 2009, when they supplanted Russia from the leading position in natural gas extraction. For the past forty years, following the oil crisis of the 1970s, energy security has been a major goal and a central organizational principle of the global strategy of the United States,[24] which is not only the world's largest consumer but also the largest importer of energy. In search of guarantees for the security of its energy supplies, U.S. foreign policy and military efforts were focused primarily on achieving stable access to the oil reserves in the Middle East.

In the past two decades, this strategic principle was modified into a commitment to global energy security. The world energy centers were the hubs where the United States concentrated their diplomatic and military efforts. There are numerous examples: sanctioning energy-producing countries such as Iraq and Libya; two major wars in the Persian Gulf; the fight against Al Qaeda, which is financed by the resources in the region to counter U.S. interests there; the attempts for Arab-Israeli peacemaking as part of the efforts to resolve the complex relationships in the region; and the commitment to protect maritime routes to Asia.

The North American shale revolution changed the picture. The immediate political effect was a reduction of U.S. dependence on oil supplies from politically uncertain regions in the Middle East and North Africa. Thus, the Middle East could be dethroned from its position of a central component in the United States' global strategy. The political discourse in the energy field is different now due to the emerging reality that transformed the United States from the world's largest energy importer into an exporter of energy resources. The year 2005 marked the peak of U.S. oil imports—60 percent of all

[22] For details, see Velichka Milina, "Energy Security and Geopolitics," *Connections: The Quarterly Journal* 6:4 (Winter 2007): 27-46.

[23] See http://www.warandpeace.ru/ru/news/view/77747/.

[24] Jon B. Alterman, "Paradigm Shift," *Middle East Notes and Comment*, Center for Strategic and International Studies (February 2013); available at http://csis.org/files/publication/0213_MENC.pdf.

U.S. domestic consumption was imported that year—while in 2012 it had already dropped to 46 percent. The reasons for this difference, of course, are to be found in increased energy efficiency and the economic crisis as well as in an increase of domestic production by 25 percent since 2008. The largest share of this increase is due to the extraction of so-called tight oil – oil that is produced by the same technology as shale gas. Expert assessments show that the volume of U.S. oil shale resources exceeds by several times the proven reserves of crude oil in Saudi Arabia.

Despite these projections, the United States still imports a greater share of its oil than in 1973, this time from providers with different geographical locations: 25 percent from Canada, 16 percent from the Persian Gulf, 11 percent from Mexico, and 9 percent from Venezuela.[25] Transforming Canada into a major exporter is quite a favorable circumstance for the security of energy supplies, as Canada is both a friendly neighboring country and the United States' largest trading partner.

Data on significant reserves in Canada as well as serious studies on the effective extraction of proven huge oil reserves in the sea territory of Brazil indicate an upsurge of oil production in the Western Hemisphere that is expected to bring a permanent rebalancing of oil in the world and will establish a new geopolitics of energy routes. Much less oil will come from the Eastern Hemisphere to the Western Hemisphere, and much more oil will flow from the Middle East to Asia. China already imports from the Persian Gulf more oil than the United States. The geography of the main countries currently exporting oil to the U.S. provides proof of the new trend of the regionalization of energy markets.

Regarding oil security, the U.S. has achieved impressive results; however, it is in the natural gas sector where we could speak of a real revolution. Strategies to export liquefied shale gas to Europe and other destinations at competitive prices are already being developed.[26] This would take both time and effort. New liquefaction facilities and terminals will have to be built so that the gas could be transported by ship across the Atlantic. For their part, European countries will also need to build LNG terminals, which do not seem a very quick solution, although the project is certainly possible with capital investment and favorable legislation.[27] Countries with such facilities will have more opportunities to diversify their sources of supply through export and import in different situations as well as through spot markets.

The development of unconventional gas production is being used by the U.S. as an instrument of foreign policy through the Global Shale Gas Initiative (GSGI), which was

[25] Daniel Yergin, "Opinion: America's New Energy Security," *Wall Street Journal* (12 December 2011); available at http://online.wsj.com/article/SB10001424052970204449804577068932026951376.html.

[26] Robert D. Kaplan, "The Geopolitics of Shale," *Stratfor Global Intelligence* (19 December 2012); available at www.stratfor.com/weekly/geopolitics-shale.

[27] The U.S. Congress was discussing a bill in December 2012 to give NATO allies access to gas supplies. Its approval will place NATO allies on an equal footing with trade partners according to U.S. legislation ensuring licenses for export of liquefied natural gas from the U.S.

launched in April 2010 by the U.S. State Department.[28] The aim is to promote the new production technology in countries that wish to identify, develop, and utilize their unconventional natural gas resources. Under this initiative, the United States has established partnerships with China, India, Poland, Ukraine, Jordan, and other countries. The objectives of this collaboration are to encourage the use of U.S. technology and win market shares in other countries; build alliances with strategic partner countries and reduce their dependence on energy imports from other countries; and promote the use of natural gas as a clean fuel and increase support for efforts to address climate change. The shale revolution has defined new positions for the U.S. on the global energy markets that they will have to master.

Russia

Russia is by far the biggest loser under the new conditions in the energy market. They portend an end to its position as an energy superpower in which the "energy card" was its monopolistic geopolitical weapon. The shale boom is bad news for Russia and, although Gazprom tried to ignore it for a long time, it is now a factor that must be taken into consideration in Russia's national policy while the country is trying to maintain its presence as a major player in the global energy markets.

For Russia, the consequences of the shale boom are direct and indirect. The ten-year contract for supplies of liquefied natural gas from Gazprom to the U.S. has been terminated. The development of the vast "Shtockman" gas field in the Barents Sea—a USD 40 billion project as part of this contract—has been suspended.

Currently, Russia is facing relatively low competition on the European gas market, as it exports natural gas in large quantities to the West and tries to use its supplies destined for Central and Eastern Europe as a tool to wield political influence. It exports over 60 percent of the natural gas used in countries such as Austria, Bulgaria, Czech Republic, Estonia, Finland, Latvia, Lithuania, Poland, Slovakia, Moldova, Turkey, and Ukraine.

However, Russian dominance is no longer unchallenged. The amounts of liquefied gas available on the market have pushed Gazprom to reduce contract prices because of the possible alternative that many European countries (Finland, Latvia, Lithuania, and Poland) may choose to build their own LNG terminals. In addition, the time when the U.S. will export liquefied shale gas to Europe is not that far off.[29]

[28] Frank Umbach and Maximilian Kuhn, "Unconventional Gas Resources: A Transatlantic Shale Alliance?" in *Transatlantic Energy Futures: Strategic Perspectives on Energy Security, Climate Change and New Technologies in Europe and the United States*, ed. David Koranyi (Washington, D.C.: Center for Transatlantic Relations, Johns Hopkins University–SAIS, January 2012), 207-228; available at http://www.bpb.de/system/files/dokument_pdf/Transatlantic-UG-Kuhn-Umbach 1211.pdf.

[29] In March 2013, a twenty-year contract was signed for U.S. shale gas supplies to the U.K. starting in 2018. See Fiona Harvey, "US Shale Gas to Heat British Homes Within Five Years," *The Guardian* (25 March 2013); available at www.theguardian.com/environment/2013/mar/25/us-shale-gas-british-homes-five-years.

Russian energy valences may realistically decrease due to the efficient development of proven substantial deposits of unconventional gas in Germany, Ukraine, the United Kingdom, Hungary, Lithuania, and Romania. Even forecasts in this direction were yet another factor that unfavorably affected Gazprom, causing changes in the long-term contracts for supplies of natural gas in Europe.

The shale boom has had an impact on the non-European markets for Russian energy resources as well. On the one hand, China has discovered significant proven shale gas formations in its inner provinces, and on the other hand a number of countries in East Asia are signing supply contracts with Canada.

Which are the viable and winning policies for Russia to preserve its role on the global energy stage under the current dynamic geoenergy circumstances? The first and most crucial one is the modernization of Russia's national energy complex. With the approach of the era of "smart" energy, Russia needs to give up wasteful production methods and use of energy resources as soon as possible.

The depletion of most of the major exploited fields draws attention to Russia's reserves of unconventional hydrocarbon resources. The latest example refers to the ongoing studies by Exxon Mobil and the Russian state company Rosneft of deposits of "Bazhenov" oil in Western Siberia. These are perhaps the world's largest reserves of what is the equivalent of shale gas in the oil industry – i.e., oil from Bazhenov rocks.[30]

Russia has the largest proven technical deposits of unconventional oil. However, these huge potential reserves do not mean that a shale oil revolution will happen in Russia similar to the one in the U.S. The main reason is that Russia's technological capacities lag far behind those in the U.S. The presence of many competing firms engaged in the search for effective technologies for the extraction of unconventional oil and gas in the U.S. resulted in the birth of a new generation of high-tech and inexpensive drills, as well as new technologies such as horizontal drilling. In Russia, this sector is still in the hands of a few powerful players, most of which are closely connected with the state.

In this geoenergy context, it is obvious that with its existing tools Russia will not be able to keep its role as an energy superpower. If the country hopes to remain a key player in the energy resources market, it will have to change the parameters of its energy policy, both inside and outside the country. Now, it will have to fight for consumers' interest in its energy supplies in times of increasing competition and falling prices.

With regard to the European energy markets, Russia's winning strategy should take into consideration the following basic unfavorable factors:

- Long-term stagnation of demand in EU member countries
- Consumption growth is expected only in Turkey
- Reduction of gas consumption in the European countries of the CIS, particularly due to high prices of resources

[30] According to the most optimistic assessments, these reserves total 143 billion metric tons. This means 1 trillion barrels, or four times the reserves of Saudi Arabia, or enough to satisfy world consumption for thirty years.

- Continuous price conflicts
- Gradual increase in the requirements imposed on suppliers (third energy package of the EU)
- The volume of Russian supplies will remain stable until 2020 (within the framework of current contracts)
- Increase of supplies while preserving existing price correlations will be insignificant (mainly for non-EU countries).

There are serious risks as well as potential for Russian energy policy in the Caspian region. The most important risks are connected with:[31]

- Final energy disintegration of the post-Soviet space (infrastructure, energy flows, exchange of investments)
- Rise of political and military influence of other countries (China, Iran, Turkey, EU, U.S.)
- Militarization of the region
- Increase of environmental issues.

Given these risks, effective policies could be focused mainly on establishing a new joint energy space with multi-agent governance and use of intelligent systems, procurement of innovative energy equipment and services, and common initiatives for environmental improvement in the Caspian region.

Many expectations for market enlargement are connected with North Eastern Asia. This region holds long-term potential for the markets in Japan (20-35 billion m^3/year, due to the disaster in Fukoshima) and the Republic of Korea (10-16 billion m^3/year).[32]

China is crucial for Russia's future role as an energy supplier in the region. But the prospects are ambiguous. By 2025, the country will not be in need of Russian gas, and afterwards it will probably meet its demands through its investment projects/contracts in other energy regions or from own production. Under these circumstances, in order to occupy an important position in the Chinese energy market, Russia will have to resort to price dumping. However, its options are quite limited, due to the increasing cost of Russian gas.

As for the prospects of energy exports to other regions in the world, the realities are not promising. Traditionally, Russian policy relies on fixed energy routes; this, however, makes reaching potential new markets either inefficient or geographically impractical. At the same time, for a number of objective reasons (climatic, geological, investment,

[31] A. M. Belogorev, "Energy Problems in the Caspian Region: Risks and Potential for Russia," Fifth Caspian Energy Forum, 25 April 2012, http://www.energystrategy.ru/ab_ins/source/Belogoryev_Caspian_25.04.12.pdf (in Russian).

[32] V.V. Saenko, "Russia's Long-term Energy Strategy in the Asia-Pacific Region," Eight International Conference on "Energy Cooperation in Asia: Risks and Barriers," Irkutsk, 21-23 August 2012, http://www.energystrategy.ru/ab_ins/source/Saenko_Irkutsk_21-23.08.12.pdf (in Russian).

etc.) the production of liquefied natural gas from Russia's major fields—Vladivostok, Yamal, Shtokman, and Sakhalin—is very costly and ultimately futile.

In general, changes in the technological and geoenergy environment of Russian energy policy outline the following restrictions in the formation of Russia's future effective energy strategy:

- Regionalization of gas markets limits the potential for access beyond Europe, CIS, and North Eastern Asia
- Due to the high costs, Russia is not able to take advantage of the globalization of the liquefied natural gas markets
- Europe is not able to continue being a driving force for growth; the key goal is to keep what has been achieved on the market
- Russia has at its disposal no more than five to six years to manage to settle on the Asian market; by 2020, the large consumers (Japan, China, and India) will have negotiated arrangements for their required energy resources.

New trends and developments in global energy suggest that Russia will gradually say farewell to its role as an energy superpower. The challenge to Russian politicians and energy planners is huge. They will have to modernize Russian energy policy on the fly, so that Russia will be adequate to the upcoming age of neo-industrial energy.

The European Union

The European Union is the participant in the global energy market that is making the greatest efforts to create energy security policies, but is generating the most inefficient results. The main reason lies in the very mechanisms of making energy policy in the EU. On the one hand, as an integration organization in which member states have delegated sovereignty to the supranational European institutions, the EU produces numerous directives and regulations regarding a common energy security policy in all its dimensions, from energy diplomacy to the protection of critical energy infrastructure. On the other hand, however, these directives and regulations always have a loophole for individual policies and actions of member states under a shared understanding that, since this is an area of vital national interests, and one of the most important dimensions of national security, members will always have difficulty arriving at a consensus solution, and therefore it is in the interest of the Union to allow space for national policies. As practice shows, such policies are often in conflict with the common European energy interests.

Proof of the controversy that is built into the very foundations of the common energy policy of the EU are the provisions in the Lisbon Treaty, which represented a culmination of efforts for greater cooperation between member states in the energy sector.[33] The treaty specifies four main objectives of energy policy in the EU:

- Ensure the operation of the energy market
- Guarantee the security of supplies in the EU
- Encourage energy efficiency, energy saving, and the development of new and renewable forms of energy
- Promote the interconnection of energy networks.

In compliance with Article 122 (1) (TEFU), these goals shall be achieved in the spirit of cooperation. This solidarity clause is an attempt to institutionalize the concept of enhanced European cooperation on energy security issues. At the same time, there are provisions for decision making on energy issues by unanimous consent. For example, Article 194 (2) and (3) of the Treaty provides that solutions proposed by the EU to introduce a common system of energy taxation, or to promote the use of a specific energy technology over others, be subject to a unanimous vote by the member states, which actually effectively gives each of them the right to a veto on these proposals.

The fact that the treaty encourages enhanced cooperation at the EU level while confirming the individual rights of member states recognizes the historical contradiction within the ideology of the EU energy policy that encourages the tendency of member states to put their own national interests above those of the community. Article 2 (C) of the Lisbon Treaty makes it clear that energy is an area of shared responsibility, but in practice it supports the unanimity of the EU on general problems of energy policy (by qualified majority), while maintaining the central role of member states regarding the specifics of this process (by unanimous vote).

This basic dichotomy in decision making in the European energy policy explains its poor performance and the fact that it is a "common policy" only *de jure*, but not *de facto*. The issue is particularly relevant in the context of the radically changing terms and conditions of energy markets, where the EU's energy policy must continue to ensure energy security and economic competitiveness of the Union to prevent negative effects on climate change.

The shale revolution has already changed the European energy market before it has produced even one molecule in domestic shale fields. The main effects have been the change in Gazprom's contractual policy, opportunities to supply liquefied natural gas at competitive prices, the availability of large quantities of coal at low prices, potential for production of shale resources in Europe (Estonia produces more than 90 percent of its electricity from bituminous shale, and is now the most shale-dependent country in the

[33] For details, see Frank Groome, "From Contradiction to Cooperation: A New Legal and Diplomatic Foundation for Energy Policy in the EU," *Journal of Energy Security* (19 April 2012); available at www.ensec.org/index.php?option=com_content&view=article&id=343:from-contradiction-to-cooperation-a-new-legal-and-diplomatic-foundation-for-energy-policy-in-the-eu&catid=123:content&Itemid=389.

world).[34] The European Union could not avoid the impact of shale gas on its climate change policy. Set by Brussels in 2007, the goal for the reduction of carbon emissions was defined due to the continuous increases in fossil fuel prices, which strengthens the business arguments to invest in renewable energy. However, as natural gas prices fall around the world, it is pointless to invest in expensive subsidized forms of renewable energy. If the support for renewable energy continues, it is likely that due to its high prices European businesses will switch to environmentally harmful coal, and the EU will make a step back.

In the old paradigm, especially after the gas crisis of 2006, the main problem of European energy security was diversification, security, and reasonable prices for natural gas supplies. In other words, reduction of its high level of dependence on Russia for its natural gas supply.

As early as November 2000, the European Commission warned in a "Green Paper" that over the next twenty to thirty years, up to 70 percent of the energy consumption in the Union would be from imported resources (the level currently stands at 50 percent). The production of EU energy is expected to fall from the current level of 46 percent to 36 percent in 2020. Imports of resources will cost around EUR 350 billion, i.e. EUR 700 for each EU citizen. Moreover, the profile of gas imports in the EU remains undiversified. 84 percent of gas is imported from three countries: Russia (42 percent), Norway (24 percent), and Algeria (18 percent).

Member states have different portfolios of suppliers of gas and routes, and those with more developed gas markets pay less for imports. The average price limit for gas supplies in the U.K., Germany, and Belgium is around 35 percent lower than the price in countries that rely on a limited number of suppliers, such as Bulgaria and Lithuania. Because of inefficient infrastructure links with the remaining part of the EU, countries in Northern and Eastern Europe feel like "energy islands."

Furthermore, Europe, which is a major potential user of energy from the Caspian region, has fallen into double dependence: first, on the traditional Russian supplies, and second, on the supplies from Central Asia and the Caspian region that are controlled by Russia. Nearly one-third of total EU imports of gas actually arrive in the EU through Russian pipelines and as a result of Russian gas swaps with the countries from Central Asia and the Caspian region.[35] In this context, the key problem for the EU and its member states regarding energy security remains its almost total dependence on Russia for its supplies of natural gas.

[34] Gary Peach, "Estonia's Shale Oil Market: How the Small Country Is Hoping to Revolutionize the Energy Sector," *Huffington Post* (30 May 2013); available at www.huffingtonpost.com/2013/05/30/estonia-shale-oil-drilling_n_3357830.htm.

[35] For more on EU gas dependence here and above see Maximilian Kuhn and Frank Umbach, "The Geoeconomic and Geopolitical Implications of Unconventional Gas in Europe," *Journal of Energy Security* (08 August 2011); available at www.ensec.org/index.php?option=com_content&view=article&id=320:the-geoeconomic-and-geopolitical-implications-of-unconventional-gas-in-europe&catid=118:content&Itemid=376.

All in all, none of the many potential solutions to resolve this key issue has been realized yet, from the construction of a southern energy corridor to the connection of the energy routes of the member states, which is the prerequisite for an integrated energy market. One of the main reasons is that investments in the energy sector are at historically low levels. According to the *Energy Roadmap 2050* produced by the European Commission, the transition to secure and competitive low carbon energy requires sustainable increases in investment in energy equipment, networks, transportation technologies, infrastructure, and efficient buildings. These higher investments are valued as equal to 1.5 percent of the GDP on an annual basis for the entire period until 2050. By 2020, the EU will need investments of about EUR 1 trillion in order to guarantee security of supplies, diversification of sources, ecologically clean energy, and competitive prices in the framework of an integrated energy market.[36]

It could not be expected that the countries of the European Union will replicate the "miracle" of the U.S. shale boom to solve the problems of monopoly dependency and energy resource prices. The reasons are of a practical nature (geology, law, population density, environment, non-integrated energy infrastructure) and the reticent attitude of societies in many European countries with regard to the effects of current technologies for the extraction of shale resources. What could definitely be argued at the moment is that approaches to unconventional resources will vary considerably between member states, who will set their own priorities in the energy sector.

In the current situation in the gas market, which is marked by a decrease of consumption in the EU, a global gas glut, the decoupling of gas prices from oil prices, and falling prices for LNG in the spot market, the European energy security policy must be seriously reconsidered. It is hardly realistic to believe that the EU needs all of the fixed routes for natural gas that are under discussion. In search of efficiency, we must rely on the most economical gas pipelines and build the optimum number of regasification terminals. What is absolutely necessary for the European energy market is to link energy infrastructures in a general reversible network to ensure security of supplies and uniform prices within the Union.

China

China's economy has the fastest growing rate of energy consumption of any economy in the world. Along with India, it is a major player in the energy market whose presence and active role in the allocation of resources affects all other countries' decisions.

The shale revolution has had an impact on China's geopolitical positions. The decrease in the significance of the Middle East for energy supplies to the U.S. was followed by declaring a new geopolitical strategy in the Obama doctrine – the "pivot to Asia." This meant a concentration of forces and strategic partnerships in the Pacific region, where the growing influence of China is a fact. The United States announced the withdrawal of aircraft patrolling the Persian Gulf and the transfer of some of them to the Pacific. For China, this means that it will need to invest more resources for security in

[36] *Challenges and Politics in the Energy Sector*.

the region and for sea routes (the Chinese fleet is already in the Indian Ocean), since 46 percent of its oil supplies come from producers in the Middle East, mainly Saudi Arabia, Iran, Kuwait, and increasingly Iraq.

The energy geopolitics of China continues to be oriented towards the Central Asian region, where it imposes the country's interests through an investment expansion that is displacing Russia from its traditional zones of influence. The exploitation of a pipeline from Kazakhstan and a gas pipeline from Turkmenistan guarantees secure supplies as opposed to sea routes.

Some of the resource sources for China are quite risky. The events in Libya caused serious losses in Chinese investments there. Iran continues to be a significant supplier of oil to China (third place) despite U.S. sanctions and diplomatic threats. Investments are increasing in Iraq, where the Chinese giant CNPC bought Exxon's share in the giant field West Qurna-1. The deposit is of strategic importance since it can provide direct supplies by sea to China via the port of Basra.

The geography of the supply sources for China is very broad. There are thirty exporting countries: 56 percent of the supplies come from the Middle East (Saudi Arabia has the largest share); 27 percent come from Africa; 13.5 percent from Asia and the Asia-Pacific region; and 3.5 percent from Latin America.[37] The China National Petroleum Corporation (CNPC), China Petroleum & Chemical Corporation (Sinopec), and China National Offshore Oil Corporation (CNOOC) are the national oil giants responsible for ensuring energy supplies to the country. They make huge investments in Africa, Brazil, and Central Asia. Part of the competitive advantage that helps them to dominate over other private oil companies includes "development activities" supported by the Chinese government. They vary from infrastructure construction and provision of development loans to building petrochemical refineries in return for the privilege to explore and buy energy assets. These investments not only provide stable energy supplies to China, they also help to maintain and increase its strategic influence throughout the world. The Chinese government also offers loans for exploration and production in exchange for ensuring ongoing oil exports. These loans have proven to be a trump card in tenders for energy contracts.[38]

With regard to natural gas, China is ambitious to diversify its energy mix by increasing its share from a modest 4 percent in 2010 to the still unimpressive 7 percent in 2020.[39] According to expectations, part of this will happen at the expense of production

[37] Iveta Frolova, "Chinese Expansion in post-Soviet Space," *Geopolitics* 2 (2013); available at http://geopolitica.eu/spisanie-geopolitika-broi-2-2013/1413-kitayskata-ekspanziya-v-postsavetskoto-prostranstvo.

[38] Aditya Malhotra, "Chinese Inroads into Central Asia: Focus on Oil and Gas," *Journal of Energy Security* (20 November 2012); available at http://www.ensec.org/index.php?option=com_content&view=article&id=387:chinese-inroads-into-central-asia-focus-on-oil-and-gas&catid=130:issue-content&Itemid=405.

[39] See "Why There's No Shale Revolution in China?" *DarikFinance.bg*, 25 January 2013, http://darikfinance.bg.

of its own shale gas,[40] even more so since according to the U.S. Energy Information Agency China ranks first in alleged technical reserves.

Geological studies have shown, however, that these gas formations are located much deeper than those that have been developed in the United States. Furthermore, the fields are in much more difficult terrain, and prospective reserves are located in mountainous areas or densely populated areas. This makes drilling for natural gas harder, and results in prices that would be approximately two to three times higher than those in the U.S.

Another barrier to the shale gas revolution in China are regulations. The state is the owner of the gas transfer infrastructure, and the market is also dominated by state players. This hampers competition and private investments that might bring development and effectiveness on the market (a problem similar to the one in Russia). The new energy context has presented China with new opportunities for its energy policy, and it will have to take advantage of them fully.

OPEC

OPEC is clearly among those players that are directly affected by the shale revolution. It is expected that the increase in oil production in the U.S. will have a serious impact on the market in general, and the Organization of Petroleum Exporting Countries must change their strategy under the new conditions.

The visible effect of the news about shale oil is the disagreement between the members of the cartel on what should their reaction be. The participants who are most dependent on oil prices suggest that production and supply be reduced in order to raise prices when they start to fall. Algeria, Venezuela, and Iran require higher oil prices to cover their internal costs and falling yields. Therefore, they are often in conflict with the Persian Gulf states led by Saudi Arabia, who have sufficient financial strength to withstand some decline in prices. African countries (such as Algeria and Nigeria) suffer most from the shale revolution, since their oil is similar in quality to the shale oil. It is they who will bear the heavy consequences from the shale revolution in the U.S.

Taking into account the expected production in the U.S. and Canada, it is estimated that by 2015 OPEC will be forced to cut its daily production by 6 million barrels in order to prevent a collapse in prices. The price issue is very important. For OPEC members, a “fair” price is around USD 100 a barrel. Lately, it has been based on the budgetary needs of the members of the cartel whose appetite for petrodollars increased significantly after the so-called Arab Spring. Hoping to avoid the fate of the leaderships in Egypt and Tunisia, the regimes in the Persian Gulf generously give gifts and subsidies in their countries. Saudi Arabia, for example, nearly doubled its budget because of such programs. Most Saudis are working for the bloated public sector, where wages are two to three times higher than those in the private sector. Another surprising fact is that Saudi Arabia ranks sixth in the world in crude oil consumption, ahead of major industrial countries like Germany, South Korea, and Canada. At the current rate of consump-

[40] In November 2009, China signed an agreement on cooperation with the U.S. regarding shale gas projects.

tion of energy resources, by the end of the decade Saudi Arabia will overtake Russia and India. To keep its system intact, the Saudi government will need to generate higher and higher revenues from oil sales. The history of Saudi Arabia is more or less the same as the history of the other members of the cartel. Iran, Iraq, Venezuela, and Nigeria also insist on higher oil prices.

The technology applied by the cartel is to reduce yield and cause a rise in prices until the so-called "fair price" is reached. The problem is that in 2004 the "fair" price for OPEC was USD 25 a barrel. Two years later, USD 50 was considered the "ideal price." Now it is USD 100. With the advance of U.S. shale oil, the organization obviously plans to go the same way: keeping prices high by controlling oil production. In the past four decades, the world GDP grew fourteen times, the number of automobiles increased four times, and the global consumption of crude oil doubled. However, OPEC, sitting on top of three-fourths of the conventional global reserves, has preserved its contribution to the market unchanged.[41]

According to BP analysts, however, the average price for a barrel will fall to USD 80 by the end of this decade. OPEC will at some point have to accept the fact that the time when it played the key role on the oil market is a thing of the past.

The New Paradigm

In the context of the old paradigm, energy security was directly related to energy independence. The idea was that if a country was self-sufficient in energy resources to a significant degree, and had an efficient (energy-saving) economy, this was supposed to lead to lower energy prices. The reality of oil prices in the U.S. after the shale boom proved that it was a utopia. The reason is that oil is a replaceable commodity whose price is determined on the world market. The price of a barrel of oil is more or less equal for each user, and when the price rises, it rises for everyone, regardless of where the supply of raw materials comes from.

Achieving energy self-reliance is practically impossible.[42] Even countries like Russia, Saudi Arabia, Venezuela, Brazil, and Canada, who are rich in hydrocarbon resources, import part of their energy as refined oil products due to insufficient capacity for refinement. This dependence could theoretically be eliminated with a little effort and investment in new plants, but this does not happen in practice. Out of the world's top ten economies, only two—Brazil and Canada—can theoretically reach complete energy independence. The others—e.g. China, Japan, and Germany—are poor in resources in

[41] Gal Luft and Anne Korin, "The Folly of Energy Independence," *American Interest* (July/August 2012); available at www.the-american-interest.com/article.cfm?piece=1266; and Gal Luft, "The Energy-Security Paradox," *The National Interest* (28 March 2013); available at http://nationalinterest.org/commentary/the-energy-security-paradox-8281.

[42] Gal Luft, "Energy Self-Sufficiency: Reality or Fantasy?" *Journal of Energy Security* (21 November 2012); available at http://www.ensec.org/index.php?option=com_content&view=article&id=394:energy-self-sufficiency-reality-or-fantasy&catid=130:issue-content&Itemid=405.

terms of their needs, which predetermines their dependence on energy imports. The radical solution is to change the paradigm, to not focus on energy self-sufficiency but rather on the reduction of the strategic importance of oil for the economy, and particularly for transport.

A 2009 book by Anne Korin and Gal Luft titled *Turning Oil Into Salt* elaborates on the popular idea that, just as salt exerted a significant impact on world history for centuries, given its role as the only effective mode of food preservation (salt wars were waged), today petroleum plays a strategic role due to its essential function as a transport fuel.[43] The solution is similar to the story of salt—oil must become a regular commodity through opening fuel competition. Just as it does not matter what kind of energy is used for the production of electricity, transport vehicles and the fuel distribution system must be open to a diverse mix of fuels. This is in the spirit of the upcoming neo-industrial age where some steps have already been made, even though this is still in the early stages – electrical vehicles, hybrid electric cars, methanol, etc.

It is important that the new paradigm highlight the understanding that the depletion of hydrocarbon resources is not imminent. This used to be a basic explanatory model in the context of the old paradigm, where innovations in energy were expected to occur with the decline of the hydrocarbon era. The shale revolution has confirmed the understanding that technological developments will create new opportunities for the efficient extraction of previously "frozen" hydrocarbon resources. A relevant example is the announcement by the Japanese state-owned Japan Oil, Gas, and Metals National Corporation (JOGMEC) on the successful extraction of gas from methane hydrate, known as "burning ice."[44] This is the first major breakthrough after decades in which researchers had tried to arrive at a method for the commercial production of this gas that exists in the sea depths in quantities sufficient to meet the demands of mankind for centuries. Since such black swans, or strategic shocks, cannot be predicted, the philosophy of innovative thinking in the energy sector needs to be changed, and environmental and highly efficient technologies must be implemented, such as the systems for Integrated Gasification Combined Cycle (IGCC), also called "clean coal." IGCC is a gasification process used for the conversion of coal and other heavy fuels into high-energy fuels, also called "synthetic gas," or "singases" for short. These gases are then purified and used in efficient combined cycle systems for the production of power. Another example of high technology is Carbon Capture & Storage (CCS), a method for capturing and storing carbon dioxide. It involves capturing CO2 emissions from large industrial plants—such as power stations, refineries, and chemical plants—and their safe storage underground.

NATO is also in the process of changing the paradigm of energy security in the context of its responsibilities. The current paradigm includes fuel efficiency and responsi-

[43] Gal Luft and Anne Korin, *Turning Oil into Salt: Energy Independence Through Fuel Choice* (Charleston, SC: BookSurge Publishing, 2009).

[44] "Japan Starts the Production of 'Burning Ice'," *Capital* (18 March 2013); available at www.capital.bg/politika_i_ikonomika/2013/03/18/2024927_iaponiia_zapochva_dobiv_na_goriasht_led/.

bility for the security of important energy routes. What is new is the turn to high technologies to achieve the objectives of energy security. A good example is the introduction to NATO of the Microgrids system, which is defined as a tool to improve the stability of the power system.[45]

Microgrids are an example of NATO's contribution to energy security, and could be defined as an integrated energy system consisting of distributed energy resources and multiple electrical loads operating as an independent autonomous grid, in parallel, or "isolated" from the basic electrical grid. Microgrids have two important overlapping features from a military perspective: diversity of sources (natural gas, diesel, oil, wind, solar, methane, etc.) to produce electricity for military bases (both at home and under severe conditions during operations), and continuity of service separate from the main electrical grid.

Revolutionary changes in the facts and circumstances of energy security call for a paradigm change that must be reflected in energy security policy. These changes must be in line with new energy technologies and the changing assessments of resource deposits. We are now on the threshold of the transition to a post-industrial, "smart" energy system, which means "smart" grids, alternative energy sources for transport, decentralizing energy, integration of energy into the techno-sphere, accompanied by increases in energy efficiency. All of this will provide for lowering the geopolitical and environmental risks and will create new opportunities for the end user.

[45] Michael Hallett, "Microgrids: A Smart Defense Based NATO Contribution to Energy Security," *Journal of Energy Security* (20 November 2012); available at www.ensec.org/index.php?option=com_content&view=article&id=390:microgrids-a-smart-defense-based-nato-contribution-to-energy-security&catid=130:issue-content&Itemid=405. P. Asmus, "Why Microgrids Are Inevitable," *Distributed Energy* (September–October 2011); available at www.distributedenergy.com/DE/Articles/15471.aspx.

The Young and the Normless: Al Qaeda's Ideological Recruitment of Western Extremists

Thérèse Postel [*]

The Boston Marathon bombings on 15 April 2013 brought terror to the finish line of one of the United States' oldest athletic events, and returned terrorism to the forefront of the United States' psyche. The world watched as Massachusetts law enforcement agencies shut down a large swath of the state in order to find a bomber on the run. As the dust settled, it was clear that a well-adjusted, popular, intelligent young man who was a naturalized U.S. citizen, from a Chechen refugee family, executed one of the most infamous terror attacks on American soil since 11 September 2001, under the wing of his older brother.

Dzhokhar Tsarnaev, a college student at the University of Massachusetts-Dartmouth, was found hiding in a boat four days after the bombing in Watertown, Massachusetts, and was subsequently arrested; he has since pled "not guilty" to all charges levied against him.[1] Dzhokhar's brother, Tamerlan Tsarnaev, was run over and killed by Dzhokhar as they attempted to flee law enforcement in the early morning hours of 19 April 2013.[2] Tamerlan was a potential American success story that went off the rails, not as well adjusted as his brother Dzhokhar, who was fondly known as "Jahar" to most of his friends and teachers. Tamerlan was an accomplished boxer, who lost his way shortly after his dreams to be an Olympian for the United States were curtailed because he was not a citizen.[3] Their parents filed for divorce, their sisters moved away, and the family life of these two boys disintegrated.[4] Soon after, Dzhokhar became a United States citi-

[*] Thérèse Postel is a native of Queens, NY. She holds a Bachelor's degree from Drew University and a Master's degree from The Milano School of International Affairs, Management, and Urban Policy. Ms. Postel currently works for the New York City Office of Emergency Management. The views expressed in this paper are solely her own and do not reflect those of any employer.

[1] Richard Oppel and Jess Bidgood, "Marathon Bombing Suspect, in First Court Appearance, Pleads Not Guilty," *The New York Times* (10 July 2013); available at www.nytimes.com/2013/07/11/us/in-court-for-first-time-boston-bombing-suspect-will-face-victims.html?_r=0.

[2] Kevin Cullen, "New Details on Wild Shootout with Bomb Suspects in Watertown," *Boston Globe* (21 April 2013).

[3] Lance Madden, "Boston Marathon Bombing Suspect No. 1 Tamerlan Tsarnaev Trained to Box for U.S.," *Forbes* (19 April 2013).

[4] Josh Gerstein, "Boston Bombing Suspects' Parents Granted Divorce in 2011," *Politico.com* (22 April 2013); available at http://www.politico.com/blogs/under-the-radar/2013/04/boston-bombing-suspects-parents-granted-divorce-in-162313.html.

zen, continued onto college, and dabbled in drugs,[5] while Tamerlan floundered in all aspects of his life.

How did the lives of two men, who showed such early promise, go so far astray? This question has laid heavily on the minds of those trying to make sense of this bombing and looking to prevent the next one. The answer is not as simple or straightforward as it has been portrayed. Last year, I completed my M.A. thesis on Al Qaeda's recruitment of Western extremists. I broke down Al Qaeda and its affiliates' recruitment patterns into three categories: structural, institutional, and ideological relationships. While structural and institutional connections between those seeking to join or act on behalf of Al Qaeda's worldview are often very concrete, ideological connections are porous and fluid. It was through this ideological avenue that the Tsarnaev brothers became radicalized.

It is of the utmost importance to understand the ideological influences and relationships that can push young individuals to become radicalized. The similarity through which hate groups, including white supremacists, far right extremists, and fundamentalist religious groups like Al Qaeda entice individuals to act violently on the group's behalf is most instructive for counter-radicalization and counterterrorism purposes.

The complete details of Tamerlan Tsarnaev's radicalization remain unclear. However, recent developments in this case show that while the primary impetus for the Boston bombing was radical Salafi jihadist literature of the kind promulgated by Al Qaeda, Tamerlan had also become immersed in other extremist right wing ideologies of the United States.[6] In a similarly twisted manner, Anders Breivik, who carried out the massacre of children at a summer camp outside Oslo in July 2011, admitted he admired Al Qaeda's ideology, persistence, and success although he was a noted white supremacist and Islamophobe. Breivic called Al Qaeda the "most successful revolutionary movement in the world" and claimed he hoped to create a "European Al Qaeda."[7] The cross-pollination and similarity of ideas between these extreme views could no longer be ignored. Counterterrorism efforts will be enhanced and bolstered if experts better understand the type of individual that is susceptible to the ideology espoused by groups like Al Qaeda.

The title of this journal, *Connections*, is very appropriate, as I believe the ideology Al Qaeda and the assortment of right-wing hate groups in the United States put forth is most appealing to those who lack sustaining connections in their life. This article will first illustrate how the extremist ideology of far-right groups and the ideology of Al Qaeda resonates with the same pool of disaffected, disconnected individuals looking for

[5] Chris Kirk and Heather Brady, "From Wrestling Captain to Terrorism Suspect: A Timeline of Dzhokhar Tsarnaev's Life," *Slate.com* (23 April 2013); available at http://www.slate.com/articles/news_and_politics/map_of_the_week/2013/04/timeline_boston_bombing_suspect_dzhokhar_tsarnaev_s_life.html.

[6] Alan Cullison, "Boston Bombing Suspect Was Steeped in Conspiracies," *The Wall Street Journal* (6 August 2013); available at http://online.wsj.com/article/SB10001424127887323420604578649830782219440.html.

[7] Richard Orange, "Al Qaeda Rejects Anders Behring Breivik Comparison," *The Telegraph* (3 May 2012).

meaning and a sense of community in their lives, using many of the same methods. The overwhelming evidence suggests this was the case for Tamerlan Tsarnaev. The importance of these connections to the radicalization process allows me to argue against the prevalence of "lone-wolf" discourse in counterterrorism today. Next, the article will further describe Al Qaeda's ideological recruitment of individuals like the Tsarnaev brothers to their apocalyptic worldview through the case study of Zachary Chesser, a young American man who tried, unsuccessfully, to travel to Somalia to join Al Qaeda in 2010. The Tsarnaev brothers are featured prominently in the May 2013 issue of *Inspire*,[8] Al Qaeda's English language magazine, which only months earlier provided them with instructions and motivation for their attack. Understanding this process of radicalization, for any type of terrorist group, may prevent loss of life by interdicting future terrorists before they are able to carry out any violent acts.

Radical Recruiting: Different Ideologies Pulling on the Same Strings

There is little theoretical research that attempts to explain Al Qaeda's recruitment tactics.[9] Perhaps this dearth of information on recruitment is a result of the group's shadowy, secretive nature. This may also be a result of the lack of experts studying how Al Qaeda recruits new adherents. Outside of the literature on Al Qaeda's recruitment patterns, there has been a significant amount of research regarding the recruitment of members of U.S. domestic hate groups. Al Qaeda and hate groups use similar rhetoric and target similarly disaffected individuals.

One can come closer to understanding the framework through which Al Qaeda attempts to recruit its members by analyzing the theory that aims to explain the recruitment methods used by right-wing hate groups in the United States. It is important to note that Al Qaeda propaganda, like *Inspire* magazine, seeks to recruit individuals passively through indoctrination, as do some domestic hate groups. Similarly, by reviewing theories regarding the nature of terrorism in the post-9/11 world, one can understand the ideological recruitment themes upon which Al Qaeda bases its narrative.

According to the Southern Poverty Law Center, there are over one thousand active hate groups in the United States.[10] Many of these groups themselves produce domestic terrorists. Prior to 9/11, the most successful terrorist attack on the United States was that of the bombing of the Alfred P. Murray Federal Building in Oklahoma City in 1995. Timothy McVeigh, although not a part of any particular hate group, was virulently anti-government and had been accused of anti-Semitic rhetoric.[11] The United States is much

[8] *Inspire Magazine*, Issue 11 (May 2013).

[9] "Al Qaeda," throughout this essay, refers to any group or individual that adheres to Al Qaeda's worldview and goals, whether or not there is a formal affiliation to the organization founded by Osama bin Laden.

[10] Southern Poverty Law Center, "Hate Map," available at www.splcenter.org/get-informed/hate-map.

[11] "Timothy McVeigh," *CNN* (29 March 2001); available at http://asia.cnn.com/2001/US/03/29/profile.mcveigh/index.html.

more familiar with the concept of domestic terrorism because of these hate groups. These groups primarily recruit individuals in three ways. First, they target individuals who are experiencing "anomie" or "strain" in their lives; these individuals who are "frustrated" with their position in society are at risk of succumbing to hate groups.[12] Second, hate groups will preach that the "status quo" is under attack, and that people must join these groups in order to protect their ethnic or religious groups' position of power in society.[13] Third, many of these groups will use "apocalyptic" rhetoric in order to recruit individuals. Many individuals believe their specific community is under attack and will be recruited into hate groups when they believe their struggle is one of destiny or is God's will.[14]

Randy Blazak documents the recruitment of neo-Nazi skinheads in his essay "White Boys to Terrorist Men." White supremacist groups in the United States recruit young individuals to their cause through several means that are similar to the way other terrorist groups recruit individuals. Blazak documents how these skinhead groups "target specific youth populations" using ideology that appeals to disaffected young people.[15] Blazak argues that individuals who experience anomie, or "normlessness," are especially vulnerable to skinhead recruitment.[16]

Recruiters for skinhead movements, as well as other race-based hate movements in the United States, tap into feelings of "frustration, anger, and a need to resolve some perceived inequity."[17] Young individuals who suffer from "a sense of rootlessness or normlessness" are more likely to join these groups in order to create an identity for themselves.[18] Skinhead groups will create a narrative of attack on the "cultural supremacy of heterosexual white men" in order to recruit young men in areas where this status quo is perceived to be under threat.[19] According to Blazak, there is a theme of "cultural crisis" in the skinhead community and our nation at large.[20] Many of these themes resonate particularly with skinheads – and, in an entirely different context, with those sympathetic to Al Qaeda. These themes are: the uncertainty of "modern life," rampant consumerism, and the "cult of individualism" in American society.[21] Fear of the "cult of individualism" is not only seen in Western society, but in many countries around the world, where people worry that globalization is bringing these vices to their societies as well. These themes, coupled with the strain of "normlessness" that at-risk youth experience, allow individuals to be recruited into terrorist groups.

[12] Randy Blazak, "White Boys to Terrorist Men: Target Recruitment of Nazi Skinheads," *American Behavioral Scientist* 44:6 (2001): 982–1000.

[13] Ibid.

[14] Ibid.

[15] Ibid., 982.

[16] Ibid., 986.

[17] Ibid.

[18] Ibid., 987.

[19] Ibid., 988.

[20] Ibid., 997.

[21] Ibid.

Perhaps most importantly, a divine and apocalyptic narrative is often used to recruit individuals. Hate groups in the U.S. claim that they are "doing God's work to save the White race from extinction."[22] Individuals recruited by these skinhead groups are swayed by the desire to "restore" white hegemony. A sense of community is formed through believing they are the "chosen few" who will win a race war, establishing a homeland for the Aryan peoples in the Northwest United States.[23] It is in this desire to reclaim a mythical era of white dominance that one sees the most striking parallels with jihadist groups.[24] Blazak notes that skinheads and white supremacist movements believe that a "race war" will bring about a homeland only for whites in the United States.[25] This narrative is deployed to recruit individuals that experience "normlessness" in their lives, and who have few other compelling attachments. Skinhead recruits see threats to their identity as white males in society today as the perceived status quo changes.

White supremacists seem to target and appeal to individuals experiencing normlessness in their lives and promise them the restoration of their centrality in society, while delivering benefits of belonging to a community. These groups recruit alienated individuals and provide them with a sense of community based upon ethnic or religious ties. Individuals are called to defend this community, and are often convinced that it is a religious duty to do so, or that their community is taking part in a mythical or apocalyptic struggle. As we will see below, Al Qaeda uses a very similar ideology to that employed by neo-Nazi groups, and exploits the same ties to community and religion.

Interestingly, the BBC and the *Wall Street Journal* have recently uncovered reports that Tamerlan Tsarnaev, although surely motivated by Salafi jihadism in the months before the Boston attack, had closely studied far-right ideology.[26] Tamerlan often took care of an elderly neighborhood man, Donald Larking, for whom his mother served as a home health aide.[27] Larking supplied Tamerlan with a copy of *The Protocols of the Elders of Zion*, a favorite anti-Semitic screed of Al Qaeda and Nazi sympathizers.[28] Tamerlan allegedly subscribed to several white supremacist newsletters, including *The American Free Press* (noted by the Southern Poverty Law Center for its anti-Semitic content) and *The First Freedom*, which advocates "equal right for whites," a topic often discussed in right-wing extremist circles who fear changes in U.S. society.[29] Tamerlan also

[22] Ibid., 983.

[23] Ibid., 994.

[24] Ibid.

[25] Ibid., 986.

[26] Hilary Andersson, "Tamerlan Tsarnaev Had Right-Wing Extremist Literature," *BBC News* (5 August 2013); available at http://www.bbc.co.uk/news/world-us-canada-23541341.

[27] Conor Simpson, "Meet the Man Who Supplied Tamerlan Tsarnaev with Right Wing Literature," *The Atlantic Wire* (6 August 2013); available at http://www.theatlanticwire.com/national/2013/08/meet-man-who-gave-tamerlan-tsarnaev-his-right-wing-literature/68020/.

[28] Cullison, "Boston Bombing Suspect Was Steeped in Conspiracies."

[29] Ibid.

possessed a piece of literature about the "rape of our gun rights," a common fear in right-wing extremist discourse.[30]

While this right-wing extremist literature seems to have played a role in shaping Tamerlan's thoughts, he was most likely indoctrinated to Salafi jihadism during his trip to Dagestan and in his prior interactions with his mother, who had become hyperreligious along with her son.[31] Through Tamerlan Tsarnaev, one can see how both white supremacists, the conspiracy theories spread by the far right in the U.S., and Salafi jihadist views could affect someone experiencing significant "strain" or "anomie" in their lives.

Salafi jihadism, known colloquially as "Islamic extremism," took a central place in the Western national security discourse after the events of 11 September 2001. As such, much of the literature devoted to the study of terrorism today speaks of the divergence between "old" terrorism and "new" terrorism. This debate is important to consider when analyzing Al Qaeda and Salafi jihadism. Many scholars believe that Al Qaeda and those who act on their behalf are the harbinger of a "new" form of terrorism, and hold that the "old" terrorism was political, state-sponsored, and less violent than the "new" terrorism espoused by Al Qaeda. However, this is a highly problematic distinction. Al Qaeda and affiliated terrorist groups today may have changed their tactics, but terrorism remains the same. Understanding that Al Qaeda does not represent a "new" form of terrorism and is politically motivated—as were all terrorist groups that preceded it—will affect the way the United States conducts its counterterrorism efforts. The United States will fail to counteract, and may even bolster, Al Qaeda's political rhetoric if scholars continue to insist that Al Qaeda represents an entirely new form of terrorism and therefore is not politically motivated. The debate between scholars regarding "old" and "new" terrorism is integral to the discussion regarding Al Qaeda's ideological recruitment strategies.

Scholars Richard Devetak, Steven Simon, and Daniel Benjamin believe that Al Qaeda before, on, and after 9/11 represented a "new" era of terrorism.[32] Simon and Benjamin argue that the first characteristic of the older form of terrorism was its political goals, which hinged on the weakening of other powers in the international system.[33] The second characteristic of the "old" terrorism, according to these scholars, is its "predominantly state-sponsored" nature.[34] In the early 1990s, terrorism was a product of nation-states—namely "Iran, Iraq, Cuba, Libya, North Korea, and China"—that sponsored terrorist groups and used them as instruments to pursue national goals.[35] The last characteristic that defines the older form terrorism was its focus on garnering attention rather

[30] Ibid.

[31] Alan Cullison, Paul Sonne, David George-Cosh, and Anton Troianovski, "Turn to Religion Split Suspects' Home," *The Wall Street Journal* (22 April 2013); available at http://online.wsj.com/article/SB10001424127887324235304578437131250259170.html.

[32] Richard Devetak, "Violence, Order, and Terror," in *International Society and Its Critics*, ed. Alex J. Bellamy (Oxford: Oxford Scholarship Online, 2005), 232.

[33] Steven Simon and Daniel Benjamin, "America and New Terrorism," *Survival* 42:1 (2000): 65.

[34] Ibid., 59.

[35] Ibid., 61.

than taking lives.[36] Benjamin states that the violence of the "old" terrorism was "carefully targeted and proportionate in scope" in order to avoid alienating people. Similarly, Devetak agrees that violence was never the "sole tactic" of earlier terrorist groups, and argues that it was used sparingly. These scholars agree that these three characteristics have been altered to create the putatively new form of terrorism executed by Al Qaeda and its affiliates.

These scholars maintain that the "new" terrorism has left its political, state-sponsored, and less violent nature behind in favor of new characteristics. According to Simon and Benjamin, the "new" terrorism is less political in nature and has instead taken on a religious motivation. These terrorists are required to carry out God's will to create a perfect world on the "cosmic stage."[37] Next, the "new" terrorists show a disregard for innocent life and aim for greater lethality in their attacks. The theological justification for their actions allows the "new" terrorists, especially Al Qaeda, to pursue "warfare without end."[38]According to Devetak, because these newer terrorist groups have no "negotiable political demands," they seek primarily to eliminate all opposition to their goals.[39]

Finally, terrorism is no longer seen as state-sponsored, but rather as operating organically through a "hub and spoke structure."[40] Simon and Benjamin observe that Al Qaeda and other "new" terrorist groups do not rely on states for financing under this analysis, but receive funding from wealthy donors, personal holdings, and donations.[41] These perceived changes in funding, motivation, and tactics represent a significant change from "old" to "new" terrorism to these scholars. However, it becomes apparent that, while there might have been a change in actors, the tactics used by terrorist groups have remained largely the same. The better explanation for the apparent change is that, like any other actor with political goals, Al Qaeda's strategies have changed as situations and contexts have changed.

More importantly, there are three fundamental errors these scholars make when drawing a distinction between "new" versus "old" terrorism. The first is an assumption that the religious goals put forth by terrorist groups cannot be political at the same time. Those who adhere to Al Qaeda's religious teachings believe that Islam itself can serve as the basis for the new "social, political, and economic order" of the new society they seek to establish.[42] Al Qaeda considers Islam a "revolutionary ideology" that unites global Islamic society.[43] The religious justification that Al Qaeda and similar groups claim for their actions is not recognized for what it truly is: a justification for the political "strug-

[36] Ibid., 65.

[37] Ibid., 66.

[38] Ibid., 68.

[39] Devetak, "Violence, Order, and Terror," 240.

[40] Simon and Benjamin, "America and New Terrorism," 68.

[41] Ibid., 71.

[42] John Turner, "From Cottage Industry to International Organisation: The Evolution of Salafi-Jihadism and the Emergence of the Al Qaeda Ideology," *Terrorism and Political Violence* 22 (2010): 542.

[43] Ibid., 549.

gle for dominance within the Islamic world."[44] This is not a "clash of civilizations," as many scholars would suggest. Rather, Al Qaeda is striving toward political goals that its opponents can combat and refute. Also, once we view Al Qaeda as a political movement, we can argue that the problem is not Islam, but rather a group of individuals who are distorting Islam for political gain.

In the same way, scholars believe that the "new" terrorism is marked by a level of disregard for human life. This misconception is based upon a misreading of terrorist groups' ideology. Al Qaeda and its affiliates believe that those working alongside dominant forces in the Middle East are "apostates," and are thus guilty. Devetak and other scholars tread in dangerous water by saying terrorists refute "humanist values";[45] placing Western "norms" on these groups leads to a flawed analysis of these groups' motivations and goals. Al Qaeda and terrorist groups do not believe that they target "innocents," but rather that they are fighting against aggressors. It is important to understand Al Qaeda's rationale in order to analyze their ability to recruit individuals.

Finally, these scholars overlook the role states still play in terrorist activity. State sponsorship of terrorism might not be as direct as it once was, but there is still significant proof that Pakistan, Iran, and even Saudi Arabia continue to support terrorism.[46] These scholars also fail to realize that terrorist groups today need a physical space from which to operate, and therefore Afghanistan, Pakistan, Yemen, and Somalia play an integral role in their operations.[47] Terrorist groups may be less hierarchical than they were in the past, but this does not mean that states have no impact or relevance on terrorist activities.

The Tsarnaevs are not an example of state-sponsored terrorism. However, Tamerlan's radicalization took place during his six months in Dagestan, a Russian province with an ongoing insurgency against the central government. The brothers' motivations have still not been explicitly spelled out, but they were clearly scarred by their displacement as children and the continued strife in their homeland of Chechnya; their immigrant status contributed to their feelings of normlessness. These pressures caused them to experience strain and anomie in their own lives, and helped them fall prey to Al Qaeda's political ideas regarding the protection of the *umma* (the global community of Islam). These ideas are not a wellspring for a "new" form of terrorism; in fact, Tamerlan's consumption of both right-wing extremist literature and his devotion to Salafi jihadist propaganda on YouTube shows that these seemingly distinct political narratives can occupy common mental ground in young individuals who are feeling isolated and alone.

[44] Ibid., 542.

[45] Devetak, "Violence, Order, and Terror," 240.

[46] Daniel L. Byman, "The Changing Nature of State Sponsorship of Terrorism," Saban Center for Middle East Policy at the Brookings Institution, Analysis Paper No. 16 (May 2008), 8, 12, 21; available at www.brookings.edu/research/papers/2008/05/terrorism-byman.

[47] Stuart Elden, "Territorial Integrity and the War on Terror," *Environment and Planning* 37:12 (2005): 2083–104.

It is important to dispel the false dichotomy of "old" versus "new" terrorism when analyzing the recruitment patterns of Al Qaeda in the United States and the West. Misunderstanding Al Qaeda and its affiliates' political goals, ideology, and need for an unstable state from which to operate and continue recruitment hinders our understanding of the avenues through which Westerners come to join Al Qaeda.

The Tsarnaevs' Thoughts: Ideological Recruitment by Al Qaeda and its Affiliates

One of the most prominent ways in which Al Qaeda and its affiliates radicalize an individual is through ideological means. Al Qaeda's ideology can be deployed to create an impression of a "war of ideas" that can be extremely salient to individuals who are experiencing strain or anomie in their lives. Tamerlan Tsarnaev struggled with school, never fit into a social group, witnessed his parents divorce and return to Russia, and saw his Olympic dreams to box as an American crushed.[48] These experiences left him disaffected and alone. In a photo essay titled "Will Box for Passport" by Johannes Hirn, Tamerlan said, "I don't have a single American friend, I don't understand them."[49] Al Qaeda's ideology helped him gain a sense of belonging to something larger than himself: the *umma*.

His brother, Dzhokhar, struggled in college to maintain the same academic and social prowess that had distinguished him in high school, and he too began to embrace radical Salafi jihadist thought as a way to cement his connection with his brother.[50] Dzhokhar's indictment asserts that he downloaded several Salafi jihadist sermons and statements from clerics Abdullah Azzam and Anwar al-Awlaki that spoke about the protection of "Muslim lands" from the hands of disbelievers. This is in line with another statement that Dzhokhar scrawled in the boat in which he was found – "The US government is killing our innocent civilians," presumably referring to the *umma*.[51] Al Qaeda not only employs religious rhetoric, but also has espoused political goals that connect with a specific constituency. It is important to note that these goals were of interest to the target populations for several decades before Al Qaeda formally came into existence.

To set the stage, one must understand that Al Qaeda embodies an ideology that has existed within the Islamic world for centuries. Osama bin Laden articulated Al Qaeda's ideology before the attacks of September 2001 in several pronouncements. He claimed the United States, its allies in the West, and conspirator regimes in the Middle East were

[48] Janeit Reitman, "Jahar's World." *Rolling Stone* (17 July 2013), 9; available at www.rollingstone.com/culture/news/jahars-world-20130717.

[49] David Weigel, "Tamerlan Tsarnaev, Dead Bombing Suspect: 'I Don't Have a Single American Friend'," *Slate* (19 April 2013); available at www.slate.com/blogs/weigel/2013/04/19/tamerlan_tsarnaev_dead_bombing_suspect_i_don_t_have_a_single_american_friend.html.

[50] Reitman, "Jahar's World."

[51] Denise Lavoie and Tom Hays, "Dzhokhar Tsarnaev, Boston Bombing Suspect, Was Influenced By Internet: Indictment," *The Huffington Post* (28 June 2013); available at www.huffingtonpost.com/2013/06/28/dzohkhar-tsarnaev-internet-indictment_n_3515432.html.

conducting a "crusade" against the *umma*.[52] Bin Laden called on Muslims across the globe to wage "defensive jihad" against the United States and its allies, as the United States was an occupier in the holy land of Saudi Arabia.[53] This war between the West and the Islamic world would be fought to reestablish a "pious caliphate" that would be governed by Islamic law and politics.[54] This blend of religion and politics is not new in Islam. In fact, a father of Al Qaeda's ideology is Ibn Tamiyya, a thirteenth-century scholar who refused to accept the "subordination of religion to politics" for those of Islamic faith.[55] A miniscule minority of individuals harbors this ideology; however, there are enough people who ascribe to Al Qaeda's Islamist ideological stances that the approach has served as a strong recruitment tool for this group since their inception. Al Qaeda's ideology, as we know, often bases itself in religious rhetoric and uses Islam as a justification for its violent actions. Scholars often dismiss Al Qaeda as a purely fringe religious movement, while others claim that Islam has current of violence, which Al Qaeda channels and magnifies to become a conduit for hate. However, what these scholars fail to acknowledge is that Al Qaeda is a fusion of a political and a religious movement. Although Al Qaeda's rhetoric may be religious, they embrace a political ideology and pursue political goals. After all, at its heart, "terrorism is a form of political violence."[56]

Richard Devetak argues that many terrorist attacks, including those which Al Qaeda has perpetrated, have a "hyperreligious motivation."[57] These acts may be framed by religious rhetoric, but they remain political at their core. Al Qaeda seeks to change the political landscape throughout the world, by replacing the Hobbesian social contract between the ruler and the ruled with a contract between God and his people, based on *Sharia* law.[58] Al Qaeda has constructed a narrative that is steeped in religion, and uses this religious motivation to bring about political action through an emphasis on selected parts of Islamic history and the Quran. Al Qaeda tells its followers, and those it hopes to recruit, that there will need to be a "violent struggle to remake the world."[59] The same rhetoric was described earlier in our discussion of neo-Nazi skinhead recruitment. White supremacists in the United States look to establish an "Aryan homeland" in the Northwestern United States, while Al Qaeda hopes to restore the Islamic Caliphate.[60] Al Qaeda's struggle is a religious duty, but there is no question that it has a political end.

[52] Christopher M. Blanchard, *Al Qaeda: Statements and Evolving Ideology*, CRS Report for Congress RL32759 (Washington, D.C.: Congressional Research Service, 9 July 2007), 3; available at www.fas.org/sgp/crs/terror/RL32759.pdf.

[53] Ibid.

[54] Ibid.

[55] Turner, "From Cottage Industry to International Organization," 549.

[56] Devetak, "Violence, Order, and Terror," 232.

[57] Ibid.

[58] Ibid., 239.

[59] Ibid., 240.

[60] Blazak, "White Boys to Terrorist Men," 994.

Mark Juergensmayer, who speaks of a "Cosmic War"[61] between Islam and the West, describes Al Qaeda's ideology as "religionised politics."[62] Al Qaeda's rhetoric may seem apocalyptic, but it is steeped in the desire to bring about a change in the status quo. As was discussed earlier, this desire to bring about social change when one's community is being unfairly targeted, attacked, or suppressed is designed to appeal to individuals who are experiencing anomie in their lives.[63] It is clear that Al Qaeda's religiously tinged political goals resonate with Muslim individuals in the West who feel as if Islam and their culture have been under attack for centuries. Al Qaeda uses this rhetoric to appeal to those who hope to restore their own version of the "status quo" – a return to power of the Islamic caliphate after years of Western dominance in the Middle East.[64]

The Tsarnaev brothers' Chechen identity is steeped in this region's struggle against Russia as an occupying power. It is easy to see how these young men extrapolated connections between Russian dominance over the predominantly Muslim provinces of Chechnya and Dagestan and the United States' "imperialist" agenda against Muslims around the globe. Tamerlan was steeped in this message during his time in Dagestan as he visited local Salafist mosques with his cousin, Magomed Kartashov, who is a prominent Islamist in the Dagestani capital of Makhachkala.[65] Kartashov's group, the "Union of the Just," renounces violence publicly, but speaks virulently about U.S. interventionism, specifically in the Middle East, and the exportation of liberal thought.[66] Although Tamerlan was also well versed in extremist right-wing discourse, this physical, ideological indoctrination into Salafi jihadist thought gave him a sense of belonging to the *umma*, a connection he desperately sought to quell his loneliness.

Osama bin Laden and Ayman al-Zawahiri have been successful in conveying that the global community of Muslims is mandated to fight a "defensive jihad" against the United States and its allies who are "occupying" the Middle East.[67] These leaders extend the analogy of the Crusades to this modern-day fight in an attempt to increase their historical and ideological credibility. In fact, Al Qaeda's political ideology and the terrorist tactics used to advance it are related to a "centuries old struggle for dominance within the Islamic world."[68] In espousing an Islamist view, which holds that Islam should provide the model for the political, economic, and social order, Al Qaeda's leaders are

[61] Mark Juergensmeyer, *Terror in the Mind of God: The Global Rise of Religious Violence*, 3rd ed. (Berkeley, CA: University of California Press, 2003).

[62] Devetak, "Violence, Order, and Terror," 242.

[63] Blazak, "White Boys to Terrorist Men."

[64] "Bin Laden's Fatwa," *PBS News Hour* (23 August 1996); available at www.pbs.org/newshour/updates/military/july-dec96/fatwa_1996.html.

[65] Simon Shuster, "Exclusive: Dagestani Relative of Tamerlan Tsarnaev Is a Prominent Islamist," *Time Magazine* (8 May 2013); available at world.time.com/2013/05/08/exclusive-cousin-who-became-close-to-tamerlan-tsarnaev-in-dagestan-is-a-prominent-islamist/.

[66] Ibid.

[67] Michael Scheuer, *Through Our Enemies' Eyes: Osama Bin Laden, Radical Islam, and the Future of America* (Washington, D.C.: Potomac, 2006), 54.

[68] Turner, "From Cottage Industry to International Organization," 542.

making a fundamentally political argument about the nature of the future state that they hope to create through jihad.

The Internet and Al Qaeda Indoctrination

In August of 1996, Osama bin Laden issued a *fatwa* titled "Declaration of War Against the Americans Occupying the Land of the Two Holy Places."[69] A *fatwa* is a binding, religious edict issued by a figure of religious authority in Islam. However, because there is no hierarchical structure in Islam, many individuals believe they are in the position to issue *fatwas*. In bin Laden's statement, he made the case that the "people of Islam have suffered from aggression" brought about by the U.S. and the "Zionist-Crusader alliance."[70] It is clear that bin Laden was looking to correct the series of humiliations that had befallen the Islamic world since the end of the Ottoman Empire.[71] Earlier, I noted that white supremacists often recruit individuals to their ranks by insisting that their position in society is under attack and has to be secured. In the same way, Al Qaeda and its affiliates create a narrative that the *umma* is being violently oppressed, and that the occupation of the lands of the Islamic Caliphate must be freed for this wrong to be corrected.[72] Increasingly, it turns to online forums to spread this message.

The Internet is an extremely important tool for the ideological indoctrination of Al Qaeda recruits in the West. Many recruits are subjected to ideological recruitment through person-to-person interaction. However, Al Qaeda has managed to create an Internet conglomerate that is easily accessed by thousands of individuals in the West.[73] Al Qaeda has established several well-known Internet chat forums, including "Al Shumukh" and "al-Fida,"[74] which operate on a "gaming" system.[75] This system gives individuals incentive to remain in the chat rooms by awarding points and rewards for their posts; this system also encourages further radicalization. According to Jarett Brachman and Alix Levine of *Foreign Policy*, "The majority of Westerners following a radical interpretation of Islam who have been arrested on terrorism charges have either been active in the hard-line forums or in possession of extremist materials downloaded from the

[69] "Bin Laden's Fatwa."

[70] Ibid.

[71] Ibid.

[72] Ibid.

[73] Brian M. Jenkins, "Is Al Qaeda's Internet Strategy Working?" RAND Corporation, Testimony presented before the U.S. House of Representatives Homeland Security Committee, Subcommittee on Counterterrorism and Intelligence (6 December 2011); available at www.rand.org/content/dam/rand/pubs/testimonies/2011/RAND_CT371.pdf.

[74] Ellen Nakashima and Joby Warrick, "Al Qaeda's Online Forums Go Dark for Extended Period," *Washington Post* (2 April 2012); available at http://www.washingtonpost.com/world/national-security/al-qaedas-online-forums-go-dark-for-extended-period/2012/04/02/gIQAfd4xqS_story.html.

[75] Jarrett Brachman and Alex Levine, "The World of Holy Warcraft," *Foreign Policy* (13 April 2011); available at www.foreignpolicy.com/articles/2011/04/13/the_world_of_holy_warcraft.

web."[76] The strongest case study for ideological Internet radicalization, indoctrination, and an individual using the Internet to radicalize others is that of Zachary Chesser.

The Case of Zachary Chesser

Raised in suburban Virginia, Zachary Chesser converted to Islam in 2008, the summer before he entered college, as the result of an experience with a soccer team. Members of *Hizb ut-Tahrir*, a radical Uzbek Islamist political organization, sponsored the soccer team.[77] This first experience with Islam underlines the importance of recruitment through institutions, which will be discussed in a later section of this paper. Chesser's ideological recruitment and radicalization is extremely interesting because of the speed with which it took place. In less than six months his views had become so stringent that he sought out further ideological support of his radical perspective. Chesser admits he turned to the Internet because "it is simply the most dynamic and convenient form of media there is."[78] Chesser's case is one of the most telling because he has remained honest in his testimony. His own statements speak to the ideological pull he felt as he formed relationships with radical Islamists through the Internet. He said, "A Muslim who sincerely investigates their religion will find that it is an obligatory [sic] to implement Islamic law, that voting is a doubtful matter, that jihad becomes obligatory in the event that non-Muslims invade Muslim lands. This is what I found, and this is what essentially everyone finds… One who sets out to learn inevitably sees jihad as viable and preferable at some point."[79] Chesser's statement shows how, once the main points of Al Qaeda's ideology take root, individuals will attempt to participate in jihad either at home or abroad to fulfill their radicalization process.

Perhaps the most important takeaway from Chesser's radicalization is his adherence to the teachings of Anwar al-Awlaki and his correspondence with this ideological leader before Chesser's arrest in Uganda in 2010. In terms of structural recruitment, al-Awlaki was an important member of Al Qaeda in the Arabian Peninsula (AQAP) until his death in 2012. AQAP has become the most active and dangerous branch of Al Qaeda as of late.[80] However, al-Awlaki's ideological sermons and writings have acted as an important recruitment factor for individuals in the West. Also, as a native English speaker and a citizen of the United States, Awlaki was soft-spoken but preached with an authority that attracted thousands of online followers who valued his pronouncements regarding

[76] Ibid.

[77] "Zachary Chesser: A Case Study in Online Islamist Radicalization and Its Meaning for the Threat of Homegrown Terrorism," Report to the U.S. Senate Homeland Security and Governmental Affairs Committee (February 2012), 5; available at www.hsgac.senate.gov/imo/media/doc/CHESSER%20FINAL%20REPORT%281%29.pdf.

[78] Zachary Chesser, Letter to U.S. Senate Homeland Security and Governmental Affairs Committee, 6 September 2011; available in ibid.

[79] Ibid.

[80] "CIA Chief Says AQAP Most Dangerous in 'Global Jihad'," *Xinhua News* (14 September 2011); available at http://news.xinhuanet.com/english2010/world/2011-09/14/c_131136754.htm.

the religious justification for terrorism.[81] Al-Awlaki struck a chord with so many individuals because of his background as an American, his seeming piety and religious expertise, and his expert use of the Internet as a tool for recruitment. Dzhokhar Tsarnaev has admitted that he and his brother-followed al-Awlaki's sermons online.[82]

Chesser became a follower of al-Awlaki about three months after his conversion to Islam. There is no doubt that Anwar al-Awlaki provided Chesser with the ideological justification for his decision to provide material support to the Al-Shabab Islamist militants and to travel abroad to Somalia in an attempt to join this affiliate of Al Qaeda. Describing his desire to put his ideological beliefs to practical use, Chesser said, "I concluded that Al-Shabab fit the mould [sic]. Al-Awlaki simply put Al-Shabab on the radar for me."[83] Chesser traded e-mails with al-Awlaki regarding his decision to travel abroad, and al-Awlaki encouraged him to travel if he thought it would be "beneficial."[84] Chesser would engage in his own ideological recruitment of others before his attempt to travel to Somalia. After he was recruited, Chesser in turn looked to recruit others through the Internet and ideological pronouncements. This strategy of using converts as "ideological foot soldiers" is an important element of Al Qaeda's overall political strategy.

Beyond the Internet

Chesser realized the importance of ideological indoctrination in order to ensure that there would be significant recruits for Al Qaeda in the future. Chesser founded *Revolution Muslim*,[85] a site for radical Western Muslims (especially those in the United States), and he was also the author of *MujahidBlog*, which was directed toward Western Muslim recruitment.[86] Chesser realized the importance of engaging and winning the "war of ideas" against the West if Al Qaeda was to succeed.[87] For this reason, he sought to become a prolific online jihadist in line with Samir Khan (of *Inspire*) and al-Awlaki, and created a series called *Counter-Counter-Terrorism*.[88] Chesser's last essay before his arrest was titled "Raising Al Qaeda: A Look into the Long-Term Obligations of the Jihadist Movement."[89] Chesser discussed the various ideological messaging efforts Al

[81] "Zachary Chesser: A Case Study in Online Islamist Radicalization and Its Meaning for the Threat of Homegrown Terrorism," 10.

[82] Daniel Klaidman, "Exclusive: The Awlaki/Tsarnaev Connection," *The Daily Beast* (26 April 2013); available at www.thedailybeast.com/articles/2013/04/26/the-awlaki-connection.html.

[83] Zachary Chesser, Letter to U.S. Senate Homeland Security and Governmental Affairs Committee, 4 October 2011.

[84] Ibid.

[85] Christopher Anzalone, "Zachary Chesser: An American, Grassroots Jihadist Strategist on Raising the Next Generation of Al Qaeda Supporters," *Perspectives on Terrorism* 4:5 (2010): 22.

[86] "Zachary Chesser: A Case Study in Online Islamist Radicalization and Its Meaning for the Threat of Homegrown Terrorism," 16.

[87] Ibid.

[88] Ibid.

[89] Anzalone, "Zachary Chesser," 22.

Qaeda must take to survive, including the “normalization” of the idea of jihad.[90] He also spoke about developing and supporting a greater role for women in “raising” children to become members of Al Qaeda.[91]

Chesser went as far as to insist that members of Al Qaeda emulate the “domestic propaganda machine” that exists within the United States, as he believed the United States created the strongest ideological connections between the individual and the nation.[92] He suggested that Al Qaeda should mirror their message to inspire the “blind patriotism” citizens of the United States experience when rallying behind the “empty terms and loaded words” of their politicians.[93] Chesser believes that instilling this sense of “patriotism” in children will create more jihadists in the future. Despite his success online, Chesser was not content to simply become a propagandist recruiter online. He believed that travel to participate in jihad was a religious obligation and an important part of Al Qaeda’s ideology.[94]

On 10 July 2010, Chesser attempted to board a flight to Uganda with his infant son with the hopes of traveling to Somalia to join Al-Shabab.[95] As Martha Crenshaw points out, many recruits are inspired by Al Qaeda’s ideology, but it is normally not until they travel abroad that they become operational.[96] Chesser was denied access to the flight and was arrested on 21 July for attempting to provide material support to Al Shabab.[97] Chesser believed that it was his religious obligation under Islam to travel abroad to fight, but to his dismay he was barred from travelling to Somalia twice before his arrest.[98] He pled guilty to all charges and was sentenced to twenty-five years in a U.S. federal prison.[99]

No part of Zachary Chesser’s recruitment to Al Qaeda suggests that there was any degree of “lone-wolf” terrorism at play. Chesser first experienced Salafi jihadism through a social institution, a soccer team, and converted to Islam shortly thereafter. His marriage to a woman he had met on Al Qaeda’s Internet forums suggests that ideological relationships formed on the Internet can foster relationships in the real world.[100] Finally,

[90] Ibid., 23.

[91] Ibid., 25.

[92] Ibid.

[93] Ibid.

[94] Ibid., 29.

[95] “Zachary Chesser: A Case Study in Online Islamist Radicalization and Its Meaning for the Threat of Homegrown Terrorism,” 19.

[96] Martha Crenshaw, Statement Before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, Committee on Homeland Security, U.S. House of Representatives, “Hearing on Reassessing the Evolving al-Qa’ida Threat to the Homeland” (19 November 2009), 4; available at http://iis-db.stanford.edu/pubs/22749/MCrenshaw.pdf.

[97] Ibid.

[98] Anzalone, “Zachary Chesser,” 28.

[99] “Zachary Chesser: A Case Study in Online Islamist Radicalization and Its Meaning for the Threat of Homegrown Terrorism,” 25.

[100] “Wife of Virginia Man who Threatened South Park Pleads Guilty,” *Anti-Defamation League* (9 November 2010); available at www.adl.org/main_Terrorism/nzabanita_chesser.htm.

Chesser looked to travel to Somalia and participate in jihad, proving that the desire to be part of a community is a focal point of recruitment. Although Chesser operated alone, with the exception of his wife, he had greater connections both through the Internet and international community that undermine any scholarship that would suggest he was a "lone-wolf."

The Tsarnaev brothers did not operate alone; Tamerlan's radicalization was aided by his six months in Dagestan, and the brothers relied on their familial bond. While it is unknown exactly how the brothers became operational, it seems that Dzhokhar followed his brother's radicalization. Again, the importance of connections when succumbing to radical ideology cannot be overstated. The radicalization process rarely occurs in a vacuum, hence casting doubt on the narrative of "lone-wolf" terrorism.

Tamerlan's six-month trip to Dagestan undoubtedly furthered his radicalization as he met with notable Salafis and spoke freely about jihad.[101] His radicalization started, however, when his mother begged him to become more religious in an effort to stem his use of alcohol and drugs. Tamerlan became so immersed in religion that he chided his family members and even encouraged his mother to wear a hijab. Together, they became more steeped in religion, driving their family apart, as the father could not understand his son's change in behavior.[102] Tamerlan could not even fit in at his local mosque in 2009, where he had an outburst regarding a sermon that praised Martin Luther King, Jr. Those who attended the service that day in 2009 were shocked by his stunning eruption. He was told if another outburst occurred, he could not return to the mosque.[103]

Tamerlan's interactions in Dagestan pushed him toward radicalization, but those he was in contact with during his stay convinced him not to join the strife in Chechnya. Rather, they suggested he return home.[104] Cast out again, armed with reinforced views against United States intervention in the Middle East from his time in Dagestan, Tamerlan and his brother began to plan the bombings. Dzhokhar, struggling in school and increasingly isolated, latched onto his only connection still close to him. His brother was the main source of radicalization.

Together, the Tsarnaevs devoured Salafi jihadist propaganda videos on the Internet, including prophecies about a global holy war to reestablish the Islamic caliphate.[105] They discovered *Inspire*, the propaganda magazine of Al Qaeda in the Arabian Peninsula (AQAP). In these pages, the brothers found their recipe for pressure cooker bombs in an article titled "How to Make a Bomb in the Kitchen of Your Mom."[106] Perhaps more importantly, *Inspire* often encourages Westerners who desire to fight in foreign

[101] Shuster, "Exclusive: Dagestani Relative of Tamerlan Tsarnaev Is a Prominent Islamist."

[102] Cullison, Sonne, George-Cosh, and Troianovski, "Turn to Religion Split Suspects' Home."

[103] Ibid.

[104] Shuster, "Exclusive: Dagestani Relative of Tamerlan Tsarnaev Is a Prominent Islamist."

[105] Lavoie and Hays, "Dzhokhar Tsarnaev, Boston Bombing Suspect, Was Influenced By Internet."

[106] Eli Lake, "Al Qaeda's Recipe for Pressure-Cooker Bombs," *The Daily Beast* (16 April 2013); available at http://www.thedailybeast.com/articles/2013/04/16/al-qaeda-s-recipe-for-pressure-cooker-bombs.html.

wars to consider themselves the "jihadist next door" and attack in their own countries.[107] In one notable video, Adam Gahdan reminded sympathizers in the U.S. that the country is "awash with guns" that are "easily attainable." The video ends ominously, asking the viewer, "So what are you waiting for?"[108] This type of propaganda aided the brothers in their path to violence.

Zachary Chesser's rapid radicalization through ideological relationships and recruitment, starting on a soccer team but becoming cemented through Al Qaeda's Internet forums, is an important case study for the United States. Chesser realized the importance of the ideological foundations of Al Qaeda's recruitment machine, and attempted to improve the longevity and reach of these recruitment measures through his own writing. His only mistake was becoming so prolific in both his writing and his desire to recruit others to the jihadist cause that he tipped off authorities to his plans, leading to his arrest. However, through the efforts of propagandists like Chesser—and the now infamous Anwar al-Awlaki and his Yemeni cohorts, who continue to publish *Inspire Magazine*—many disaffected young men like the Tsarnaevs are at risk of falling prey to Al Qaeda's radical world view.

The Tsarnaevs themselves, although they had no tangible connections to any arm of Al Qaeda, succumbed to this ideology and committed a horrific act of violence that left three young people dead and hundreds injured on a beautiful day in Boston. The success of Al Qaeda's ideological recruitment and propaganda has garnered the Tsarnaevs a starring role in the latest edition of *Inspire*, released in May 2013.[109] On the first page of the magazine, Al Qaeda offers, "Americans, you should understand this simple equation: as you kill, you will be killed. Yesterday it was Baghdad, today it is Boston." *Inspire* claims "the two great brothers," Tamerlan and Dzhokhar, as Al Qaeda's own, even though their connection to this movement was purely ideological. Tamerlan is pictured in a heavenly scene, dressed in his flashy clothes from his boxing days and a pair of aviator sunglasses. *Inspire* calls on all "true" Western Muslims to follow the lead of the Tsarnaev brothers. The glorification of the Tsarnaevs through online forums and chat rooms that make discussing future plots and religious zeal a game, with points and ranks, has begun.[110] Alienated individuals will find satisfying ties to this community, and the cycle may begin again.

[107] *Inspire Magazine*, Issue 10 (March 2013).

[108] Sam Stein, "White House Taking 'Seriously' Al Qaeda's Eying of America's Gun Show Loophole," *The Huffington Post* (7 June 2011); available at www.huffingtonpost.com/2011/06/07/white-house-taking-seriously-al-qaeda-gun-show_n_872413.html.

[109] *Inspire Magazine*, Issue 11 (June 2013).

[110] Brachman and Levine, "The World of Holy Warcraft."

Conclusion

Dzhokhar Tsarnaev's next hearing in federal court is on 23 September 2013. At the time of this writing, he plans to plead "not guilty" on all counts.[111] Regardless of the outcome in court, there are important conclusions to be drawn from the Tsarnaevs' radicalization, especially in Tamerlan's process. Tamerlan experienced great normlessness and anomie in his life, so much so that he confessed openly he did not have "one American friend." This sense of rootlessness, driven by his troubled childhood and inability to fit in to any social group, allowed him to be swayed by right-wing extremist, white supremacist, and Salafi jihadist ideology. The sense of purpose and community these ideologies lend to individuals experiencing disconnection from society is an area that should be explored more by academics and counterterrorism professionals. Perhaps, if the FBI had recognized these characteristics in Tamerlan when they interviewed him in the summer of 2011 at the behest of the Russian government, his radicalization could have been halted.[112]

Tamerlan's radicalization was aided by the relationships he formed in Dagestan, his bond with his mother, and his connection to his brother Dzhokhar. These relationships pushed the brothers to become increasingly radicalized. Their relationship to Al Qaeda's ideology, as well as their belief in protecting the *umma* (as evidenced by Dzhokhar's note inside the boat), highlight the importance of establishing societal connections during the radicalization process. Radicalization, whether it takes place via the Internet or in person, rarely occurs in a vacuum. The fear of "lone-wolf" terrorism is overblown for these reasons. Instead, counterterrorism and law enforcement should focus on interceding with those who are experiencing anomie in their lives.

Finally, the importance of Al Qaeda's propaganda machine for ideological indoctrination and recruitment cannot be overstated. Through the case study of Zachary Chesser, I have illustrated how individuals can be radicalized solely through the online community. Chesser understood the importance of recruiting online, and Al Qaeda is aware that at-risk, lonely youth are easily swayed by their radical propaganda, which can be easily found on the Internet in sermons and on the pages of *Inspire*. The Boston marathon bombings bring this narrative full circle. The Tsarnaev brothers, disaffected and alone, acted on their violent beliefs, fostered by *Inspire* magazine, and now play a starring role in the May 2013 edition.

As the United States looks to stop the next Western extremist before they become operational, the ideological path of the Tsarnaev brothers, especially Tamerlan, is instructive. Scholars may speak in meaningless clichés like "Al Qaeda 3.0," but in truth, this type of radicalization is all too common in the United States and has been for dec-

[111] Oppel and Bidgood, "Marathon Bombing Suspect, in First Court Appearance, Pleads Not Guilty."

[112] "2011 Request for Information on Tamerlan Tsarnaev from Foreign Government," Federal Bureau of Investigation National Press Release, 19 April 2013; available at www.fbi.gov/news/pressrel/press-releases/2011-request-for-information-on-tamerlan-tsarnaev-from-foreign-government.

ades.[113] In the case of Tamerlan, one can see a lonely, disaffected young man who became immersed in all types of extreme ideology – he just happened to cultivate the personal relationships that pushed him toward Salafi jihadism. In order to stop the next terrorist, the United States should recognize that both the white supremacist terrorist attack on a Sikh Temple in Wisconsin in August 2012 and the Boston bombings are less about the narrative that takes hold and more about the social state of these attackers that led them to seek out a radical ideology.[114] This would be a fundamental change in our approach to counterterrorism as a nation, but it is one idea whose time has come.

[113] Bruce Riedel, "Al Qaeda 3.0: Terrorism's Emergent New Power Bases," *The Daily Beast* (3 December 2012); available at http://www.thedailybeast.com/articles/2012/12/03/al-qaeda-3-0-terrorism-s-emergent-new-power-bases.html.

[114] Brendan O'Brien, "Vigil at Wisconsin Sikh Temple Marks Anniversary of Shooting Attack," *Reuters* (6 August 2013); available at www.reuters.com/article/2013/08/06/us-usa-shooting-sikh-idUSBRE97505320130806.

Connections: The Quarterly Journal

Submission and Style Guidelines

Connections accepts manuscripts in the range of 2,000 to 5,000 words, written in a lucid style for a target audience of informed defense and security affairs practitioners and academics. All manuscripts should be submitted to the *Connections* editorial office electronically at PfPCpublications@marshallcenter.org. They should feature the author's name, current institutional affiliation, and a provisional title at the top of the first page, and should include footnotes where necessary.

Preferred themes for the FY 2014 publication year include:

Cyber Security
Environmental Security
Military in Crisis Management
Connected Forces Initiative
Security, Stability, and Reconstruction Operations
Good Governance in Security and Defense
Contemporary Challenges in Defense Education
Armed Non-state Groups
Border Security
Reshaping and Reforming Armed Forces

For questions on footnotes and references, please refer to the Chicago Manual of Style, at http://www.chicagomanualofstyle.org/tools_citationguide.html.

Unsolicited manuscripts are accepted on a rolling basis at the discretion of the PfPC Editorial Board.

The views expressed in all CONNECTIONS publications are solely those of the contributing authors, and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

The Operations Staff of the PfP Consortium of Defense Academies and Security Studies Institutes is located at the George C. Marshall European Center for Security Studies:

Gernackerstrasse 2
Bldg. 102, Room 306B
82467 Garmisch-Partenkirchen, Germany
Phone: +49 8821 750 2333, Major Enrico Müller
E-mail: pfpconsortium@marshallcenter.org
www.connections-qj.org

For all information regarding
CONNECTIONS please contact the
PfPC Operations Staff
at:
pfpcpublications@marshallcenter.org
or by using the information above.

ISSN 1812-1098
e-ISSN 1812-2973