

CONNECTIONS

THE QUARTERLY JOURNAL

CONNECTIONS SUMMER-FALL 2021



PARTNERSHIP FOR
PEACE CONSORTIUM
OF DEFENSE
ACADEMIES AND
SECURITY STUDIES
INSTITUTES

SUMMER-FALL 2021

NETWORKS OF SOCIAL
COOPERATION

MARITIME
CYBER(IN)SECURITY

HOW TALIBAN
AND THE WORLD
SEE EACH OTHER

*Partnership for Peace Consortium of
Defense Academies and Security Studies
Institutes*

The PfP Consortium Editorial Board

Sean S. Costigan	Editor-In-Chief
Ed Clark	Managing Editor
Aida Alymbaeva	Institute for Analysis and Initiatives Development, Bishkek
Pal Dunay	George C. Marshall Center, Garmisch-Partenkirchen
Philipp Fluri	Wenzao Ursuline University (WZU) in Kaohsiung, Taiwan
Piotr Gawliczek	University of Warmia and Mazury in Olsztyn, Poland
Dinos Kerigan-Kyrou	Abertay University, Ireland
David Mussington	US Government
Chris Pallaris	i-intelligence GmbH, Zurich
Tamara Pataraiia	Caucasian Institute for Peace, Democracy and Development
Todor Tagarev	Bulgarian Academy of Sciences, Sofia
Eneken Tikk	Cyber Policy Institute, Jyväskylä, Finland

The views expressed and articles appearing 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.

This edition is supported by the United States government. 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 Partnership for Peace Consortium at PfPCpublications2@marshallcenter.org.

The Summer-Fall 2021 edition of *Connections: The Quarterly Journal* was published with delay. The content may reflect information and events more recent than the date indicated on the cover.

Dr. Raphael Perl
Executive Director

Sean S. Costigan
Editor-In-Chief and Chair, Editorial Board



ISSN 1812-1098, e-ISSN 1812-2973

CONNECTIONS

THE QUARTERLY JOURNAL

Vol. 20, no. 3-4, Summer-Fall 2021



Contents

Vol. 20, no. 3-4, Summer-Fall 2021

Research Articles

- | | |
|---|-----|
| How Networks of Social Cooperation Scale into Civilizations
<i>Hilton L. Root</i> | 5 |
| Security Aspects of Hybrid War, COVID-19 Pandemic and
Cyber-Social Vulnerabilities
<i>Chad Briggs, Yuriy Danyk, and Tamara Maliarchuk</i> | 47 |
| Maritime Cyber(in)security: A Growing Threat Imperils EU
Countries
<i>Yavor Todorov</i> | 73 |
| Security Threats of Radicalism through Social Media amid
Covid-19 Pandemic: Indonesia's Perspective
<i>Aththariq Rizki and Fauzia Gustarina Cempaka Timur</i> | 95 |
| A Reciprocal Relation: How Taliban and the World See Each
Other
<i>Mirwais Balkhi</i> | 107 |



How Networks of Social Cooperation Scale into Civilizations

Hilton L. Root

George Mason University, Schar School of Policy and Government,
<https://schar.gmu.edu>

Abstract: This article analyzes structure and function in the network design of historical regimes of China and Western Europe to build a theory for the development of societies and states from endogenous mechanisms of social change. It shows how their respective network structures evolved independently but share a global property: both are small worlds, meaning that any node in the network can reach any other node by a small number of steps. Probing the variations in network topologies and their role in diffusion and scaling, the author accounts for differences in formal institutions, interpersonal trust, cultural norms, and moral protocols. Network structure as an independent variable moves the discussion of the divergence of East and West beyond the conventional, centralized China versus decentralized Europe debate. It allows us to identify an overlooked driver of structural change in the polity, helping to discern better what sets the development of world civilizations apart.

Keywords: political economy, networks, comparative development, Europe, China, structural transformation.

Introduction

For decades, the socioeconomic models that tested cooperation predicted that it would only endure in groups that developed social norms of commitment, trust, and reciprocity.¹ But as Mathew Jackson noted, and what still holds, those predictions invariably have drawn from models that address small groups of agents

¹ For an overview of this literature see Mark S. Granovetter, "The Impact of Social Structure on Economic Outcomes," *Journal of Economic Perspectives* 19, no. 1 (2005): 33-50, <https://doi.org/10.1257/0895330053147958>.

and ignore questions of how communities build networks into historical regimes with the capacity to create bonds extending beyond kinship and lineage.² How, for example, did the cultural and historical assemblages of Europe and China form and survive millennia? How did they become capable of coordinating complex, multilayered functions of leadership succession, property transfer, the mobilization of revenue and arms, and the development of codes of conduct and moral persuasion? The advent of agent modeling on a massive scale enables the range of the analysis to extend to large networks from which we can collect global information about structures, such as the existence of underlying small-world or scale-free characteristics.

Scholars who focus on questions of long-term cultural differences between China and the West offer rival explanations based on economic, geographic, demographic, institutional, or political interpretations, but one theme is consistent: China was centralized, and Europe decentralized.³ In this article, I examine China and Europe's economic trajectories by exploring their respective network structures and information-sharing mechanisms. Discoveries in network science have shifted the focus of social network analysis from single-node centrality and small-graph connection mapping to consideration of the large-scale properties of the graph (the network structure) itself. Researchers can now study how network mechanisms enable system-level connectivity and the diffusion of innovation for large-scale cooperation – and how the systems themselves coevolve with the communities they support. As I search for the network mechanisms that allow

² Matthew O. Jackson, *Social and Economic Networks* (Princeton: Princeton University Press, 2008).

³ The conventional view that attributes Europe's dynamism to its decentralized interstate competition is argued in: Marc Bloch, *Feudal Society* (Chicago: The University of Chicago Press, 2014), 431; Avner Greif and Guido Tabellini, "The Clan and the Corporation: Sustaining Cooperation in China and Europe," *Journal of Comparative Economics* 45, no. 1 (February 2017): 1-35, <https://doi.org/10.1016/j.jce.2016.12.003>; David S. Landes, "Why Europe and the West? Why Not China?" *The Journal of Economic Perspectives* 20, no. 2 (Spring 2006): 3-22, <https://doi.org/10.1257/jep.20.2.3>; Nathan Rosenberg and L.E. Birdzell Jr., *How the West Grew Rich. The Economic Transformation of the Industrial World* (New York: Basic Books, 1986); Joel Mokyr, *The Lever of Riches: Technological Creativity and Economic Progress* (Oxford: Oxford University Press, 1990), <https://doi.org/10.1093/acprof:oso/9780195074772.001.0001>, 231; Chiu Yu Ko, Mark Koyama, and Tuan-Hwee Sng (2018). Other prominent scholars reliant on the competitive state system vs. unified imperium paradigm include Montesquieu (trans. 1900), Karl Marx, *Division of Labour and Mechanical Workshop: Tool and Machinery*, Economic Manuscripts of 1861-63 (New York: International Publishers, 1991); Max Weber, *General Economic History* (London: Allen & Unwin, 1927); Jared M. Diamond, *Guns, Germs, and Steel: The Fates of Human Societies* (New York: W.W. Norton, 2005); Geoffrey Parker, *The Military Revolution: Military Innovation and the Rise of the West 1500-1800* (Cambridge: Cambridge University Press, 1996); Geoffrey Parker, *The Cambridge Illustrated History of Warfare: The Triumph of the West* (Cambridge: Cambridge University Press, 2008); and Immanuel Wallerstein, "The Rise of State-System: Sovereign Nation-States, Colonies and the Interstate System," in *World-Systems Analysis*, ed. Immanuel Wallerstein (Duke University Press, 2004), 42-59.

individuals and communities to engage in large-scale cooperation, I also want to find sources in network structures that help explain the diffusion of innovation. In this way, I can explore not only the shared properties of China and Europe but also the varieties of social organization that shaped their respective “innovation cultures” and permitted them to construct networks of scale to solve problems of social cooperation.⁴

A critical element of cooperation and diffusion of innovation in any network is the connectivity from one community to another. It is easy to see how modern information technologies link to the dynamics of interdependence within and among nations. Information sharing is everywhere around us. Yet, in many sparsely governed premodern polities, it was also possible for beliefs and institutions representing a unity of the collective to be woven together. Diffusion mechanisms also permitted the long-lived historical regimes in Europe and China to scale from their original tribal/village networks into broader communities, kingdoms, states, nations, and ultimately civilizations.⁵

The author proposes that long-enduring civilizations, states, and societies are of a universal class of systems whose network structures comprise many differing patterns of intersections but which share a global property: their ability to connect the parts—the hamlets, villages, and townships—and coordinate activities among them, no matter how remote or sparsely administered, through information-sharing networks that allow a collective memory and sense of common purpose. They are giant webs of communication in which, at some fundamental level, every node processes information from the other nodes that form the system. I turn to network science to explore how this information sharing came about in the absence of modern communication technologies.⁶

Western Europe and China’s network structures, or topologies, evolved independently, yet as small-world networks, any node can reach any other node in the network in a small number of steps. Their small-world connectivity itself shares another property: in both, connectivity was historically embodied in a system of rule by hereditary kingship. As I examine differences in the two network

⁴ Complex networks are explored in Fernando Vega-Redondo, *Complex Social Networks*, Econometric Society Monographs, Series Number 44 (New York: Cambridge University Press, 2007); Mark E.J. Newman, “The Structure and Function of Complex Networks,” *SIAM Review* 45, no. 2 (2003): 167-256, <https://doi.org/10.1137/S003614450342480>; and Mark Newman, Albert-László Barabási, and Duncan J. Watts, *The Structure and Dynamics of Networks*, Princeton Studies in Complexity (Princeton: Princeton University Press, 2006).

⁵ Both early Europe and China sustained complex state-based social capacity that far exceeded the longevity of the Mongol, Ottoman, or Mughal empires found in the center of Eurasia.

⁶ Information technologies link to broader national interest and international standing in contemporary political economy in *The Uses and Abuses of Weaponized Interdependence* (Daniel W. Drezner, Henry Farrell, and Abraham L. Newman, eds., *The Uses and Abuses of Weaponized Interdependence* (Washington DC: Brookings Institution Press, 2021).

structures, we will see how the diffusion of information within them afforded different advantages to each.

In Section 1, the author will explore how durable small-world networks come into being, their evolutionary convergence, and why they hold advantages for augmenting cooperation beyond the affinities of kinship and lineage. This section describes how societal structures network into complexity and includes descriptions and specific definitions of small and large worlds, concluding with a discussion of the role small-world connectivity plays in the formation of long-lived historical regimes. Section 2 addresses the system-level structures in the West and China and includes the role played by bridge nodes. The following two sections employ historical analogizing to discuss specific social institutions that support connectivity: Section 3 discusses an institution that China and the West shared, hereditary succession, and Section 4 examines institutional differences, such as religion, as well as social mobility, elite recruitment, and local governance. Section 5 explores how these network structures can also account for differing innovation systems, with inferences for the different economic structures of the two regimes. Section 6 discusses the network sources of interpersonal social trust and the embeddedness of cultural norms. The conclusion speculates on how longstanding differences in their network topologies may continue to shape the evolution of these two societies, taking into particular consideration the fact that China lacks any historical parallel to the trust-building networks and institutions that were fundamental to Western Europe's development.

Connectivity: How System Topology Enables Communities to “Network” into Complexity

The original human communities were small-scale networks built on kinship and tribal affiliation. This homophily—the tendency to associate only with similar people—enabled them to survive.⁷ Most ethnographic descriptions of early human settlements generalize that when homophily is prevalent, there also arise distinct traditions, e.g., particular gods, laws, and cultural norms. For example, some societies emphasize status by descent, while others emphasize achievement. Without shared beliefs, moral codes, or rules, the communities refrain from large-scale cooperation. Many primitive societies also maintained highly impermeable internal barriers that reinforced the stratification of members, further resulting in the disconnectedness of the whole.⁸

Yet homophily also made the greater system they inhabited a “large world,” a theoretical term reflecting the reality that communications and interactions

⁷ Miller McPherson, Lynn Smith-Lovin, and James M. Cook, “Birds of a Feather: Homophily in Social Networks,” *Annual Review of Sociology* 27 (2001): 415-444, <https://doi.org/10.1146/annurev.soc.27.1.415>.

⁸ Kent Flannery and Joyce Marcus, *The Creation of Inequality: How Our Prehistoric Ancestors Set the Stage for Monarchy, Slavery, and Empire* (Cambridge: Harvard University Press, 2012); Hilton L. Root, *Network Origins of the Global Economy: East vs. West in a Complex Systems Perspective* (Cambridge University Press, 2020), 115-119.

were primarily local and isolated. When depicted on a graph, a large-world network exhibits a high clustering coefficient but low network connectivity.^{9,10} Thus, a large-world network can be made up of nodes that cluster in sizable groupings, but each node will link to only a few nearby nodes, and communities (nodes) do not link to one another. There are no long paths to reduce distances between various nodes within this highly decentralized structure.

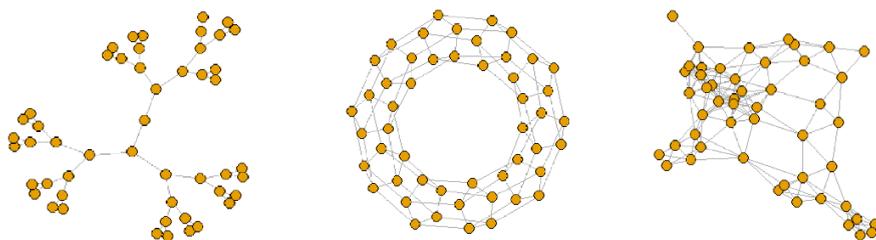


Figure 1: Three Diagrams of Large-world Networks.

These are highly decentralized systems with dense local connectivity; many steps will be necessary to move information across the system, creating a long average path length.

Where there are no long paths, there is a *long average path length*, another system-level property of large worlds. Path length is not a measure of length per se, but of efficiency. It determines how rapidly and through what channels information is distributed across the wider network. In a large world, information passes along short paths, from one node to the next and then to the next. Transmission across the entire system may require thousands of interactions between individual nodes—ergo, a long path length from any start point A to endpoint B—making diffusion costly, time-consuming, and prone to disruption and distortion. For this reason, the large world can support only limited communication, most of which stays local, and change is confined within the community where it first occurs; there was little systemic change, and what occurred would have been minuscule. Early communities were tightly clustered groups with few overlapping transactions or ties, and generated few advances in the technical or sociological environment. Evidently, being decentralized is an insufficient precondition to solve fundamental dilemmas of social coordination.

⁹ The links of small-scale networks usually show a relatively even distribution to each other and aggregate into something that resembles the network of streets or subway stations in a city, roads in the countryside, or pixels in a digital image. A network of airline flights, by contrast, is small world in that it features many connected hubs that shorten paths and improve system-wide coordination.

¹⁰ Thomas Michelitsch et al., *Fractional Dynamics on Networks and Lattices* (Wiley, 2019), <https://doi.org/10.1002/9781119608165>.

It was Granovetter¹¹ who introduced the importance “weak” ties might play because of their embedded links in social networks, and Watts and Strogatz,¹² who solved the puzzle of how to overcome local clustering constraints to enable information diffusion across a wider network. Their conceptual breakthrough, the creation of a ring model, shows how a large-world network can display both numerous local clusters, which they term its *high clustering coefficient*, and *short average path lengths* between clusters – and thus transform itself into a small-world network. They did this by adding a few random long links to bridge the circle.¹³ It takes just a few such bridges between large clusters to facilitate information flow and help spread information from any part of the network to other parts of the network.^{14,15} Introducing long paths into separate clusters, or communities, can dramatically reduce the “degrees of separation” of the population

¹¹ Mark S. Granovetter, “The Strength of Weak Ties,” *American Journal of Sociology* 78, no. 6 (1973): 1360-80, www.jstor.org/stable/2776392.

¹² Duncan J. Watts and Steven H. Strogatz, “Collective Dynamics of ‘Small-World’ Networks,” *Nature* 393 (6684) (1998): 440-42, <https://doi.org/10.1038/30918>.

¹³ The idea of “six degrees of separation,” memorialized on Broadway in the 1990s, is a small-world phenomenon common to social networks. Long before the idea became popularized, Traverse and Milgram showed that the modern communications infrastructure could be modeled as a “small world” (Jeffrey Travers and Stanley Milgram, “An Experimental Study of the Small World Problem,” *Sociometry* 32, no. 4 (December 1969): 425-43). The model assumes first-world technology. We are concerned with the communication infrastructure before electrical circuitry or steamships.

¹⁴ Albert-László Barabási, *Linked: How Everything Is Connected to Everything Else and What It Means for Business, Science, and Everyday Life* (New York: Penguin Group, 2003); Duncan J. Watts, “The ‘New’ Science of Networks,” *Annual Review of Sociology* 30 (2004): 243-70, <https://doi.org/10.1146/annurev.soc.30.020404.104342>.

¹⁵ Centola and Macy model generative mechanisms that diffuse complex contagions along complex social topologies (Damon Centola and Michael Macy, “Complex Contagions and the Weakness of Long Ties,” *American Journal of Sociology* 113, no. 3 (November 2007): 702-34, <https://doi.org/10.1086/521848>). Related work in computer science (Jon M. Kleinberg, “Navigation in a Small World,” *Nature* 406, no. 6798 (2000): 845, <https://doi.org/10.1038/35022643>), epidemiology (M. J. Keeling, “The Effects of Local Spatial Structure on Epidemiological Invasions,” *Proceedings of the Royal Society B Biological Sciences* 266, no. 1421 (1999): 859-867, <https://doi.org/10.1098/rspb.1999.0716>); and physics (Mark E.J. Newman, S.H. Strogatz, and Duncan J. Watts, “Random Graphs with Arbitrary Degree Distributions and Their Applications,” *Physical Review E* 64 (2001): 026118, <https://doi.org/10.1103/PhysRevE.64.026118>) all reveal how randomly placed long-distance links can influence social diffusion processes. Structural properties affect communication as shown by Albert, Jeong, and Barabási (Réka Albert, Hawoong Jeong, and Albert-László Barabási, “Internet: Diameter of the World-Wide Web,” *Nature* 401, no. 6749 (1999): 130-31) and Dodds, Muhamad, and Watts (Peter Sheridan Dodds, Roby Muhamad, and Duncan J. Watts, “An Experimental Study of Search in Global Social Networks,” *Science* 301 (5634) (September 2003): 827-29, <https://doi.org/10.1126/science.1081058>). Influence dynamics across virtual networks are discussed in Backstrom et al. (Lars Backstrom et al., “Group Formation in Large Social Networks: Membership, Growth, and Evolution,” In KDD’06: Proceedings of the 12th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, August 20-23, 2006, Philadelphia, Pennsylvania, USA, [10](https://www.cs.</p>
</div>
<div data-bbox=)

and thereby increase the speed of information diffusion across the greater network.¹⁶

When even a few pivotal hubs can act as bridge nodes, the long links they enable will shorten the average path length so that information can “bridge” distance and diffuse quickly. A large world becomes small when any node can reach other nodes via links and intermediate nodes. Bridges that shorten the average path length enable small worlds to form. The importance of this small-world connectivity in social organization and regime formation derives from its capacity to spread information while minimizing the number of links required to do so. The more numerous the *long* links, the more innovation can diffuse across the wider network. In this sense, states, nations, and civilizations are all different representations of a network with a small-world topology.

The historical patterns of connectivity often form macroscopic patterns of unintended order whose logic lies outside the intentions and precognition of the individual agents. Although human action is purposeful, and individuals do not make social ties at random, the actions of many can produce coherent wholes that serve important purposes without having been designed for that end.

The System-Level Structure of Social Relations in Europe and China

Watts and Strogatz¹⁷ show that a ring network transforms from a large world into a small-world network by adding a few random links to a regular network. The key to using their analysis for understanding the course of regime growth is to identify the pivotal bridge nodes or path shorteners and what they represent, the particularistic forms they may take, and the mechanisms that explain their growth.¹⁸ In the historical regimes of both China and Europe, the royal houses, secured as they were by accepted customs and rules, were the primary system spanning bridges. I map the network structure of the European leadership hierarchy and, with historical analogizing, compare it with that of China.

cornell.edu/~lars/kdd06-comm.pdf, 44-54) and Centola (Damon Centola, “The Spread of Behavior in an Online Social Network Experiment,” *Science* 329 (5996) (2010): 1194-97, <https://doi.org/10.1126/science.1185231>; Damon Centola, “An Experimental Study of Homophily in the Adoption of Health Behavior,” *Science* 334 (6060) (2011): 1269-72, <https://doi.org/10.1126/science.1207055>). Node distance is compared to the size of the network in Mitleton-Kelly, Paraskevas, and Day (Eve Mitleton-Kelly, Alexandros Paraskevas, and Christopher Day, eds., *Handbook of Research Methods in Complexity Science* (London: Edward Elgar, 2018), <https://www.e-elgar.com/shop/usd/handbook-of-research-methods-in-complexity-science-9781785364419.html>, 413).

¹⁶ Centola and Macy, “Complex Contagions and the Weakness of Long Ties.”

¹⁷ Watts and Strogatz, “Collective Dynamics of ‘Small-World’ Networks.”

¹⁸ Peter Hedström and Richard Swedberg, eds., *Social Mechanisms: An Analytical Approach to Social Theory* (Cambridge University Press, 1998), <https://doi.org/10.1017/CBO9780511663901>; Peter Hedström, *Dissecting the Social: On the Principles of Analytical Sociology* (Cambridge University Press, 2005), <https://doi.org/10.1017/CBO9780511488801>.

Figure 2.1 is a composite representation of European dynastic marriages from the fourteenth through the twentieth centuries. The network exhibits mixed features of small-world and scale-free networks. It has a highly skewed degree distribution, with a few large hubs, prevalent in scale-free models, though it is not a perfect power law distribution (Figure 2.2). It also exhibits small-world characteristics because it has an average shortest path length comparable to random networks but with a much higher clustering coefficient. In the network, communication channels to larger nodes or hubs are highly skewed, with a few highly connected hubs linking the smaller nodes with one another. Identifying these critical properties of the network helps explain why describing Europe solely in terms of decentralization gives short shrift to the patterns of hub-based communication that enabled lateral transmission across the network. We hope to better visualize how the connectivity of periphery nodes to the core nodes follows discreet patterns that produce cohesion throughout the entire network.

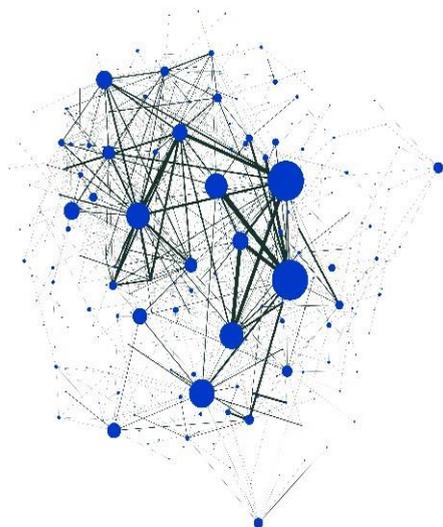


Figure 2.1: The Marriage Network between European Royal Houses from the Fourteenth through the Twentieth Centuries.

An edge is established when there is a marriage between two royal houses. The thickness of the edges represents the number of marriages between two royal houses (ranging from 1 to 92). The size of a node represents its degree, the number of houses with which it has a marriage relationship (ranging from 0 to 41). The network includes 239 nodes and 622 edges, excluding self-loops (marriages among members in the same house). The nodes also include nobility, popes, bishops, and electors. Bishops and popes were expected to be celibate, but some had children for the express purpose of establishing alliances, and these were included. The marriage network resembles a small-world network. Using Python, 100 random networks with the same number of nodes and edges are generated, and the clustering coefficient and the average shortest path are calculated for each simulated network. The European network has the average shortest path length of 3.3857, comparable to that of a random network of 3.4844, but with a much higher clustering coefficient of 0.2010 in comparison with 0.0218 of a random network.

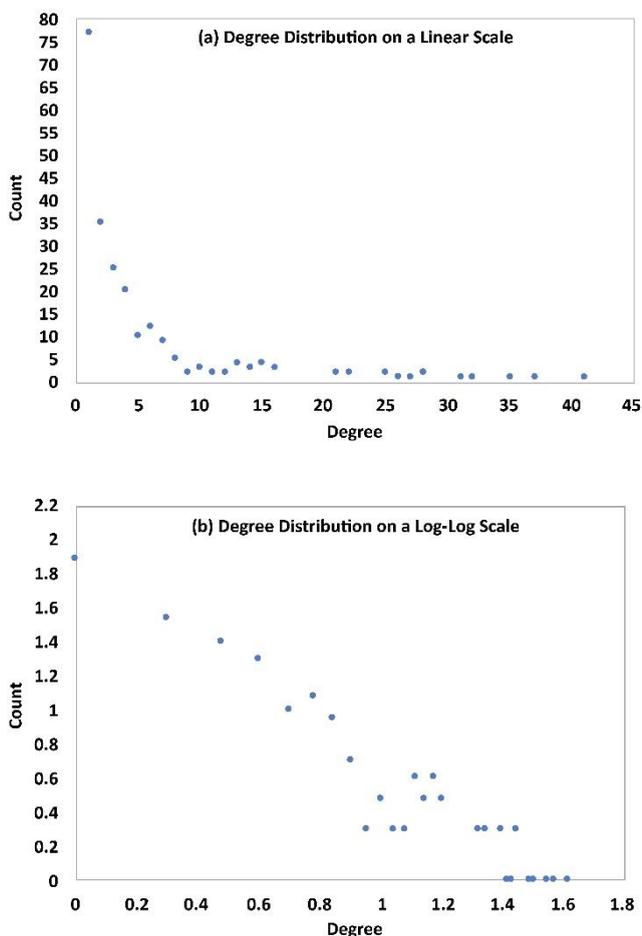


Figure 2.2: The Degree Distribution of the European Marriage Network between Royal Houses (a) on a Linear Scale, and (b) on a Log-Log Scale

The marriage network resembles a scale-free network to some degree. A scale-free network is, strictly speaking, supposed to have a highly skewed degree distribution with a long tail, following a power law distribution that is expected to be linear on a log-log scale.

Motives that Influence the Formation of Ties in Royal Networks

Distributed across Western Europe, the continent’s numerous royal houses built out macro linkages in a polycentric institutional context that relied on persuasion and alliance building to solve problems of collective action.¹⁹ This kind of *distributed network* actually gains stability by adding new nodes. Some of the nodes will

¹⁹ Elinor Ostrom, *Understanding Institutional Diversity* (Princeton University Press, 2005).

remain random, “lonely outposts,” so to speak. Some will themselves become hubs that attract numerous links throughout the system and play a critical role in its resilience. The hubs continuously change their relative importance in the system, and as each seeks advantage by attracting new nodes, system-level dynamism is amplified. To thrive, a royal lineage would have to become adept at harnessing local clustering to its advantage. Kings required the skill to assemble a patchwork of multiple jurisdictions with pledges to protect administrative, fiscal, legal, and linguistic liberties from challengers. This way of attracting potentially useful allies preserved subsidiary connectivity and a diversity of local economic contexts. Throughout medieval and early-modern European history, this process was at work, creating political boundaries and cultural identities. An unintended consequence was that as one connected cluster vied for dominance over another, innovation thrived; without the connectivity, there would not have been the same dynamism within the system.

When hubs and their accumulated nodes, i.e., communities with similar interests or functions, form subsystems without dissolving the underlying structure, this can trigger coevolutionary change. In Europe, networks bridging political and culturally disparate regions grew, enabling scientific, cultural, and technological innovation to spread across the continent. Intermittent, episodic rewiring did not fundamentally alter the defining properties of the network of international royal houses, and the network’s durability enabled economic and legal change to occur within a common European context.

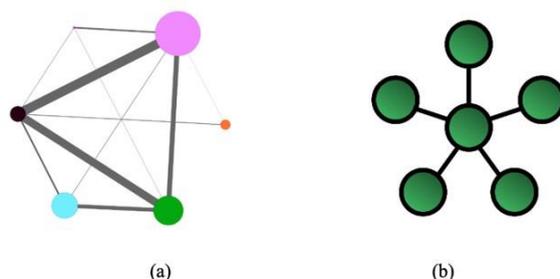


Figure 2.3: Contrasting Structure of Core-Periphery Connectivity of European and Chinese Royal Networks.

Western Europe (a) evolved into a distributed network with some nodes growing into hubs as they attracted more connections. Simplified relationships between power clusters. The node size represents betweenness centrality, or how often a given node falls along the shortest path between any two other nodes. Line thickness is proportional to the number of marriages between two houses. China’s network structure (b) resembles a star, with the emperor and court at the center controlling whether or not to share information originating from other hubs. The core-periphery structure is elaborated in more detail in the text via historical analogizing, contrasting the idealized model above with observations of network behavior from historical sources.

In China, the emperor was the central hub of a *star-shaped network*, and he alone had linkages with all other nodes. His power derived from conquest rather than alliances, giving him enhanced discretion over the network's subsequent growth processes by means of that hub-and-spoke connectivity with the periphery.²⁰ The throne was supported by the state system of Confucian officialdom, the mandarinates, which was recruited by a civil service examination system and made important official appointments, managed systemwide feedback, and transported information from one point to the next across the far-flung empire. This network structure reduces redundancies and retains resources. So, the central node can guide network growth in accordance with principles that enhance its supervision over the nodes. Its efficient top-down distribution allows rapid diffusion of approved innovations. System stability relies upon the capacity of the imperial court to perform nationwide tasks of public administration, defend its commanding position in relation to local leadership, constrain the formation of rival elites that might challenge the center, and establish regime boundaries.

Dynasty after dynasty of Chinese monarchs relied on the same recruitment, indoctrination, and examination system as a means to control the flow of ideas and preserve authority.²¹ When a dynasty collapsed by war or internal corruption, the new dynasty reinstated the examination system so that it, too, would have information brokers who spanned the empire. The network approach helps us to understand better how this civil service system contributed to the stability of imperial rule. Knowledge of small-world topology, and the reciprocal influence and coevolution of individual action and network structure, will help us infer how historical institutions are woven into the structure and to identify clues to the course of their evolution.²²

²⁰ During certain periods, the China's political unification faced challenges similar to the European experience. Just as royal administrations in Europe had to battle with the aspirations of regional elites, Chinese elites held views about centralization that were at odds with those of imperial administrators. This was especially true, economic historian Eric Jones points out, during the 9th through 13th century, when innovation in China flourished due to a sociopolitical likeness with Europe. Jones attributes this flourishing to the competition of multiple sources of institutional legitimacy that were eventually eliminated by the process of Imperial unification (Eric L. Jones, *The European Miracle: Environments, Economies and Geopolitics in the History of Europe and Asia* (Cambridge, UK: Cambridge University Press, 1981).

²¹ Frederic Wakeman Jr., *The Great Enterprise: The Manchu Reconstruction of Imperial Order in Seventeenth-Century China*, Vol. 1 (Berkeley, CA: University of California Press, 1986).

²² Individual actions and network structure coevolve in a dynamic process of reciprocal influence – see Stefano Tasselli, Martin Kilduff, and Jochen I. Menges, "The Microfoundations of Organizational Social Networks: A Review and an Agenda for Future Research," *Journal of Management* 41, no. 5 (2015): 1361-87, <https://doi.org/10.1177/0149206315573996>.

Shared Institutions in China and the West: Hereditary Succession and Primogeniture

Of note, in both China's star-shaped and Europe's more distributed network structure, there arose institutional synchronicity: hereditary lordship. In both regions, monarchs acquired the right to bequeath their status and privileges to their children, usually via primogeniture. This sets both systems apart from other known historical meta-regimes, such as the Roman, Ottoman, or Mughal empires, which failed to codify the rules for dynastic succession.²³ In regions that did not solve succession, disputes among distant relatives were more likely to end in conflict, either civil war or invasion by a rival power. In Rome, for example, while there was a general inheritance to male heirs, emperors typically chose a successor, usually a family member, sometimes an adopted heir – and the symbolic consent of the Senate and the generals was a critical factor. Neither an emperor nor his heir acquired an intrinsic “right” to rule, opening the door to contestation.²⁴

In Europe, predominant *nonroyal* social networks were also based on hereditary privilege. In China, the governing elite was selected in a recruitment system that emphasized individual achievement and, as a consequence, was more favorable to social mobility. This promotion of achievement-based bureaucracy might seem ironic if we consider that Europe developed democracy sooner. But the irony dissipates when we take into account David Bien's explorations of Old Regime France,²⁵ in which he found that democracy first developed within the privileged orders and then spread to the broader society.²⁶ Consistent with Bien's reasoning, this analysis substantiates that democratic pluralism originated in Europe's aristocratic corps and spread out over time to subsidiary systems within the larger decentralized whole. It sprang from the interplay of many competing monarchies and their ties to a subsystem of relatively autonomous aristocratic retainers, each seeking some form of collective representation in the decisions that concern the whole.

²³ While imperial rule has a 4000-year history in China, the successful usurpation from inside ended after the Sung dynasty (960-1279). From that point onward, clear rules for dynastic succession were adhered to and dynastic cycles were generally the result of external conquest.

²⁴ Keith Hopkins, “The Political Economy of the Roman Empire,” in *The Dynamics of Ancient Empires: State Power from Assyria to Byzantium*, ed. Ian Morris and Walter Scheidel Morris (Oxford: Oxford University Press, 2009), 178-204.

²⁵ Rafe Blaufarb, Michael S. Christofferson, and Darrin M. McMahon, eds., *Interpreting the Ancien Régime: David Bien* (Oxford: Voltaire Foundation, 2014).

²⁶ Noble privilege and state modernization often went hand in hand (David Bien, “Offices, Corps, and a System of State Credit: The Uses of Privilege under the Ancient Regime,” in *The French Revolution and the Creation of Modern Political Culture: The Political Culture of the Old Regime*, Vol. 1, ed. Keith Michael Baker et al. (Oxford: Pergamon Press, 1987), 89-115). Bien argues that the struggle for democracy and participation occurs within state institutions and is not only a contest of state versus society. See also Blaufarb, Christofferson, and McMahon, eds., *Interpreting the Ancien Régime*.

In both China and Western Europe, lordship succession was usually via agnatic, or patrilineal, primogeniture. In Europe, primogeniture stabilized the feudal system and facilitated its spread during the eleventh century from the polities of the former Carolingian empire, then eastward in the twelfth and thirteenth centuries.²⁷ Shielding the estates of feudal lords from fragmentation, the primogeniture system bolstered their ability to fulfill their military obligation to the king. But this geopolitical security came at the price of perpetuating the wealth, power, and social standing of noble lineages.²⁸ It also made state building and capacity dependent upon the cooperation of noble families, enabling their rights to be memorialized in constitutional settlements that constrained the scope of royal discretion. Democracy sprang from these compacts between elites and rulers. In China, such families were more likely to be viewed as potential threats to the particular imperial line. There was no institutionalization of formal consultative procedures, although there were treatises on morality and ethics like the *Ancestral Injunctions* (1375) that served for the Ming Dynasty, but these are not constitutions.²⁹

Nevertheless, hereditary lordship did not eliminate every category of disputed succession for Europe's feudal rulers. The Church had its own rules and did not tolerate divorce or concubinage or recognize illegitimate offspring. This made

²⁷ Over the course of medieval history, the former regions of the Carolingian Empire, including Aragon, Austria, Bavaria, the Duchy of Milan, Florence, France, Navarre, and Prussia, adopted primogeniture.

²⁸ The Western Church also recognized nonroyal primogeniture, thereby strengthening these elite lineages. In *An Inquiry into the Nature and Causes of the Wealth of Nations*, Adam Smith explains the political economy logic of primogeniture: "When land was considered as the means, not of subsistence merely, but of power and protection, it was thought better that it should descend undivided to one. In those disorderly times, every great landlord was a sort of petty prince. His tenants were his subjects. He was their judge, and in some respects their legislator in peace and their leader in war. He made war according to his own discretion, frequently against his neighbors, and sometimes against his sovereign. The security of a landed estate, therefore, the protection which its owner could afford to those who dwelt on it, depended upon its greatness. To divide it was to ruin it, and to expose every part of it to be oppressed and swallowed up by the incursions of its neighbors." (Adam Smith, *An Inquiry into the Nature and Causes of the Wealth of Nations*, ed. Edwin Cannan (London: Methuen & Co., 1904), 306).

²⁹ Designating clear lines of dynastic succession became an essential contribution to the formation of durable regimes and therefore to the scaling up of social complexity. In Kokkonen and Sundell, primogeniture is more stable than alternative succession arrangements in a sample of contemporary authoritarian regimes (Andrej Kokkonen and Anders Sundell, "Delivering Stability – Primogeniture and Autocratic Survival in European Monarchies 1000-1800," *American Political Science Review* 108, no. 2 (April 2014): 438-53, <http://dx.doi.org/10.1017/s000305541400015x>). The introduction of automatic hereditary succession in an autocracy limits the number of coups conducted by challenger. See Peter Kurrild-Klitgaard, "Autocratic Succession," in *The Encyclopedia of Public Choice* (Boston, MA: Springer, 2004), 358-62, https://doi.org/10.1007/978-0-306-47828-4_39.

royal lineages vulnerable if there was no male heir, creating a category of contention—female-line heirs with competing claims—that triggered frequent succession disputes and wars.³⁰

Yet, for reasons we are about to explore, European succession conflicts were generally localized without threat to the stability of the system of intermarried royal lineages that crisscrossed the continent at large.³¹ In many instances, disputes resulted in alliances between the lineages that had advanced rival claims to the unoccupied throne. Even when failure to produce an heir resulted in the extinction of an entire lineage, connectivity among the remaining royal houses would simply reroute, enabling macro-level continuity of the system.

When an imperial dynasty collapsed in China, it was usually not for lack of a male heir. Emperors could amass extensive harems to breed male successors. Concubinage contributed to intermediate regime durability, reducing the danger of a succession crisis.³² What is commonly referred to as the “dynastic cycle” would more often reassert itself when military victory swept out one dynastic line and ushered in another via rebellion or conquest. And because the peripheral nodes connected primarily through a centrally positioned hub, they too collapsed, making the repercussions far more devastating and widespread.³³ There are two key points here: Crises of dynastic succession were less frequent in China, which enabled stability and prosperity over a large territory and longer periods. On the other hand, Europe’s succession conflicts, although more frequent, were more localized and had a less dramatic effect on regime stability or on continent-

³⁰ A smooth leadership transition reduces conflicts that place existing institutional and social balance at risk with harmful effects on economic development. See Avidit Acharya and Alexander Lee, “Path Dependence in European Development: Medieval Politics, Conflict, and State Building,” *Comparative Political Studies* 52, no. 13-14 (2019): 2171-2206, <https://doi.org/10.1177/0010414019830716>. The Norman kingdom of Italy owes its decline to an inability to produce male heirs. The Hundred Years War (1337-1453) between England and France was precipitated by a dispute over female inheritance. Most succession conflicts were generally short affairs until the Wars of Religion (1562-98), which ruptured the Church and raised the stakes of obtaining the throne, adding another dimension to the quest for power since it gave royals more control over the appointment of bishops within their jurisdiction, as well as greater sway over confessional matters.

³¹ Royal families connected by living ties were less likely to fight wars. See Seth G. Benzell and Kevin Cooke, “A Network of Thrones: Kinship and Conflict in Europe, 1495-1918,” *American Economic Journal: Applied Economics* 13, no. 3 (July 2021): 102-33, <https://doi.org/10.1257/app.20180521>.

³² The longevity of Chinese rulers exceeded that of their European counterparts, providing stability and prosperity over a large territory. See Yuhua Wang, “Sons and Lovers: Political Stability in China and Europe before the Great Divergence,” *SSRN Electronic Journal* (October 2018), <http://dx.doi.org/10.2139/ssrn.3058065>.

³³ Albert-László Barabási, Réka Albert, and Hawoong Jeong, “Scale-Free Characteristics of Random Networks: The Topology of the World-Wide Web,” *Physica A: Statistical Mechanics and Its Applications* 281, no. 1-4 (2000): 69-77, [https://doi.org/10.1016/S0378-4371\(00\)00018-2](https://doi.org/10.1016/S0378-4371(00)00018-2).

wide demographic or economic trends. I revisit the long-term dynamical effects of this network property in Section 5.

The Western Church, Confucian Ethics, and the Network Dynamics of Social Change

This section is concerned with the bridge nodes that accelerate the spread of beliefs and behaviors that form notions of shared identity and common destiny. While religion played an important system-preserving and boundary-spanning role in both China and Europe, reducing the degrees of separation among socially, geographically, and culturally distant groups, it was also the source of different conceptions of political and social order that were to bear fruit over successive centuries. In terms of network structure in Europe, religion, i.e., the Roman Catholic Church, gained an institutional foothold as an independent hub in the continent's distributed network. It coevolved with other nodes, also exhibiting highly skewed degree distributions, similar to the interconnected royal families, eventually becoming a powerful force with which even the mightiest had to reckon. The span of the Church's far-reaching authority and responsibilities reached from the highest centers of power, where priests were confessors to royalty, to the local parishes, where country friars mingled with the peasantry. From the early Middle Ages, the legitimation of dynastic lordship by divine right required kings to receive holy anointment, and the Roman Catholic Church came to play a major role in the evolution of the European state system.³⁴ Although a symbiotic relationship was of benefit to both religious and secular leadership, both sides continually jockeyed to get the better of the other. As conditions fluctuated, their mutualistic relationship was held together by a shared interest in grounding the population's overarching unity upon a common faith and a desire by each lineage to avoid being compressed into a network dominated by a single lineage. Thus both lay and clerical state actors accepted and benefitted from the symbiosis of their long-term relationship.

As an institution, the Western Church enjoyed relative autonomy in recruiting its officials and running its courts and parishes according to its own procedures. During the High Middle Ages (1000-1250), "[t]he lay power might draw its authority from God, but only in subordination to the sacerdotal power embodied in its head, the Pope, the successor of St. Peter."³⁵ Secular rulers were vassals of God who exercised their dominion as servants of the Church, under the aegis of

³⁴ When Pope Leo III crowned Charlemagne Emperor of the Romans in 800, he established the precedent in the West that an emperor must be anointed by a pope, and all kings by the pope's representatives, the archbishops. A few centuries later, the coronation of William in the Norman conquest of England provides a notable but rare example of the Church according recognition to a newborn royal lineage. The difficulty of gaining Church acquiescence discouraged nonroyal challengers and made it especially difficult for a non-Christian to aspire to a European throne.

³⁵ Henry Orton Wiley, *Christian Theology*, Vol. 3 (Kansas City, MO: Beacon Hill Press, 1951), 941.

the pope, who was the Vicar of God. Since the aim of the Christian life is salvation, the *sacerdotium* occupied the higher plane, above secular rulers.

No equivalent of the Roman Church, with its independent hierarchy and sources of legitimacy, can be found in China's religious history. The emperor alone was the embodiment of Heaven's will; his mandate descended directly from Heaven. At no time was divine unction (anointment) required from an independent religious body to legitimate the investiture. Religious practice, like all other matters in China, was subordinated to the authority of the state. Even the rites of accession that sanctified the emperor's office were guided by government regulations and promulgated key elements of state ideology.

One example of such subordination developed during the Han dynasty (206-220), when a Ministry of Ceremonies, one of the nine imperial ministries, was established. The office was responsible for ceremonial observances, as well as custody of the sacred Mount Tai, recognized as a holy site for three thousand years. Ming and Qing emperors worshipped Heaven and Earth at the Temple of Heaven not far from the Forbidden City. The Ministry of Ceremonies, in effect, integrated the emperor with the natural and transcendent worlds. It also had supervision over education, which eventually included the civil service examinations. The mandarins of the imperial court, trained in classical Confucian education, alone made all important appointments to officialdom and set educational standards for the imperial university, including the appointment of academic chairs that interpreted the Confucian canons.

This subordination was reinforced by a philosophical turning point in Chinese cultural history that occurred very early on, in the fourth century BCE, with the rise and fall of Mohism, a philosophy based on the teachings of the philosopher Mo Ti (or Mozi, c. 470-c. 391 BCE). Mohism arose during the same period and from the same region as its major rival, Confucianism, during the war-torn era of the Hundred Schools of Thought. With a message of egalitarian and impartial caring for all, discouraging excessive attachment to family and clan, it had the potential to encourage individuals to invest in social organizations outside of the lineage. The tenets of Confucius prevailed, and the Confucian modeling of national community on filial piety translated into allegiance to the emperor and lent legitimacy to the throne.

Before Confucian thought proliferated throughout the empire, ancestor worship and lineage were the basis of social order, but it lacked an explicit ideology. Confucian doctrine complemented pervasive clan-based cultural norms that were widely accepted in ancient China. Because Confucianism lacked formal institutions of its own, it was readily subordinate to the state, providing a social and moral underpinning that made it appealing to the emperor.³⁶

³⁶ Zhuo Xinping, "Spiritual Accomplishment in Confucianism and Spiritual Transcendence in Christianity," In *Confucianism and Spiritual Traditions in Modern China and Beyond*, Vol. 3, ed. Fenggang Yang and Joseph Tamney (Leiden and Boston: Brill, 2011), 280-81.

Network Growth, Innovation, and Regime Longevity

Despite the small-world properties of high local connectivity and relatively short average path length shared by both China and Europe, differences in the organizational structure—the topology—shaped their respective cultures of innovation, resulting in divergent economic trajectories.

Comprised of many hubs with highly skewed degree distributions, the West's small-world network left Europe's monarchs with limited capacity to stem the spread of innovation that challenged their authority or to control systems of production that would ensure their grip over the economy. But it offered great vitality from the recurrence of revolutions and social movements, each built upon earlier accomplishments, creating something new and different, yet retaining the context of a shared European tradition.³⁷

The ability of the hierarchical linkages, beliefs, and institutions to support the hubs in accommodating rapid changes at lower levels without affecting the overall topology bolstered system-level resilience. Understanding this resilience informs us about accelerated ideological adaptations and technology diffusion that occurred via continent-wide movements, such as the Renaissance, the Reformation, the Enlightenment, and industrialization. Each started in one part of Europe, eliminating some nodes in its wake; nevertheless, the surviving hubs could self-organize into new formations. As a consequence, Europe has been more successful than China at harnessing the drivers of innovation; its interconnected governing elites are able to survive waves of cultural, institutional, and technological change, and its social development could travel far beyond where it began from the start of the Early Medieval Period, despite disruptions caused by novel social forces.

In imperial China, where systemwide connectivity emanated from the central hub, potential new hubs were discouraged from gaining footholds. Merchant guilds, charitable confraternities, and other local-level civic communities rarely gained institutional autonomy either, since new links would dilute central control. Along with limits to internal mobility via family registration in the ancient *hukou* system, this gave the central hub great capacity to determine which innovations entered the mainstream and which were to be filtered out. The *hukou* system, for example, was used to control internal migration and predated even the imperial era. Its sophisticated mechanisms for exploiting collective vulnerabilities advanced the interest of the state and its agents, but it also reduced the reservoir of potential creativity for disruptive innovation. When there was a significant shift in world views, it generally stemmed from a mandate promulgated by an imperial sponsor, often in association with a dynastic transition, rather than being a self-organizing or emergent property of agent interactions.

³⁷ Harold J. Berman, *Law and Revolution: The Formation of the Western Legal Tradition* (Cambridge, MA: Harvard University Press, 1983), 19.

The imperial court had absolute control over the mandarin state via the classical curriculum in which candidates were educated from an early age, the examination system to which they were subjected, and the regions to which they were posted. China's network distribution made unity more complete, but the cohesion of the entire network depended on the durability of the central hub. Whenever the center fell, so too did the system's remaining nodes, which were connected only to it. Each dynastic collapse meant that the bureaucracy had to be restored and the systemwide connectivity reassembled.

Yet reconstitution of the mandarin state in each dynasty is not the whole story of how Chinese cultural norms persisted over millennia. Local networks that operated on the basis of kinship and clan linkages played an essential connective role in China's history. In the next section, we will explore how such networks were possible.

Cultural Diffusion and Persistence

With network science as a methodology to discover both the global rules and change mechanisms that pervade the entire social system, I have identified an underlying dynamic of small-world connectivity at the macro level that is replicated in the historic regimes of both Europe and China. Applying the small-world approach heralded by Granovetter³⁸ and formalized by Watts and Strogatz,³⁹ the author has uncovered predominant patterns of large-scale network design, but this does not provide a full description of the system's evolution over time. Nor does it effectively account for cultural persistence. In this section, I will first examine local patterns in Europe and then disclose what the small-world approach misses as we look more deeply at China – and probe how its religious and civic institutions are linked to deep structural differences in its economic organization.

Path length within the large-scale network is key for understanding the dynamics of how information and technological change spread, i.e., as hubs form and path length within the system decreases, diffusion increases. But what about the connectivity at lower levels, i.e., among local nodes? There the successful spread of innovative behaviors requires reinforcement from multiple sources, including across community groups, requiring intersecting bonds that Damon Centola calls *bridge wideners*.⁴⁰ Individuals had to make significant investments to create these enduring pathways of social coordination across groups.⁴¹ An ideal from religion encouraged their spread.

³⁸ Granovetter, "The Strength of Weak Ties."

³⁹ Watts and Strogatz, "Collective Dynamics of 'Small-World' Networks."

⁴⁰ Social diffusion in large, complex societies may depend on socially "intermediate" groups that bind socially remote groups together. See Damon Centola, *How Behavior Spreads: The Science of Complex Contagions* (Princeton: Princeton University Press, 2018), 34-62.

⁴¹ Centola, *How Behavior Spreads*, 133.

Throughout the Medieval Period, the Church as an institution and a system of beliefs was instrumental in reinforcing new ad hoc groups for the common benefit. Fustel de Coulanges, in the mid-nineteenth century classic “The Ancient City,” explained that Christianity introduced the idea that “It was not the domestic religion of any family, the national religion of any city, or of any race. It belonged neither to caste nor to a corporation.”⁴² The idea of generalized morality made the government of medieval towns different from ancient Greece and Rome, in which every family and community worshipped its own gods. It allowed voluntary associations to flourish and build webs of organized cooperation beyond kinship. The institutional frameworks and customs they inspired supported economic opportunity in a decentralized environment.

As an advocate of norms that prescribed fairness toward strangers, the Church doctrine of brotherly love underpinned the common ideal of cities as moral communities. It shaped attitudes toward migrants and played a role in how towns dealt with migration processes, enabling strangers to obtain rights.⁴³ Common interest organizations require generalized morality to thrive. Greif and Tabellini offer an explanation for the role of Christian humanism in building the civil society of early medieval towns.⁴⁴ The networks of guilds, monastic orders, and other voluntary societies that Christian humanism inspired helped accelerate the spread of new behaviors, especially after the periods of massive migration and population replacement following the Black Death (1346-48), and enabled the towns to become seedbeds of innovative behaviors.

The multiple voluntary communities and common interest organizations, such as the *Lex mercatoria*, that built their own institutional infrastructures to manage a wide range of risks were Centola’s “bridge wideners.” The assurances they provided reduced the risk of exchanging with strangers so that groups of people who had no prior relationships could pool resources and build large private firms and markets.

China’s distinctive pattern of organizing cooperation can also be traced to longstanding historical patterns. Their relational networks became embedded and then predominant in trade and local problem solving throughout its history, even to this day. There was no body of religious thought in China that might induce individuals to trust in social ties beyond those of parochial origin like the family or village. There was no institution either that devolved from a central place like the parish that impacted the quotidian needs of the population. China’s star-shaped network structure, which relied on ancient Confucian moralism, ultimately provided inadequate formal problem-solving capacity at the local levels. The state bureaucracy was too thinly spread to penetrate local society to the level of the village, causing civil service officers to depend upon lineage leaders

⁴² Numa Denis Fustel de Coulanges, *The Ancient City: A Study on the Religion, Laws and Institutions of Greece* (Garden City, N.Y.: Doubleday and Co., 1956), 391.

⁴³ Miri Rubin, *Cities of Strangers: Making Lives in Medieval Europe* (Cambridge: Cambridge University Press, March 2020), <https://doi.org/10.1017/9781108666510>.

⁴⁴ Greif and Tabellini, “The Clan and the Corporation.”

to carry out instructions that needed local support. This resulted in negative effects on governance functions ranging from tax collection to irrigation management.⁴⁵

Cooperation or assistance via civic organization among individuals, families, and groups sharing common interests was rarely encouraged. When there was self-sponsored, self-help action by communities to solve local problems, membership was based on kinship rather than on generalized common interests. China grew relationship-based *guanxi* networks, richly endowing Chinese society with a circle culture of small groups and personal cooperation and exchange in small communities. The high moral obligations inculcated within such parochial groups rarely extended to external dealings, either with the government or, more generally, with strangers.

Assessments of kinship-intensive governance throughout the world and in contemporary settings have found that when lineage leaders held predominant roles in community organization, an inhospitable environment for behavioral innovations and cultural inertia resulted. In addition, greater kinship intensity correlates with less attention to universal morality and less generosity for those outside the group; this strengthens loyalty to family members even when they break covenants with society at large.⁴⁶ Strong in-group loyalty and a sharp distinction between in- and out-groups contribute to a general distrust of strangers with negative impacts on the quality of governance.⁴⁷

Contemporary research on China continues to find that clans sharing patrilineal ancestry are the most important social groups in Chinese villages.⁴⁸ Xu and

⁴⁵ Joseph Esherick and Mary Backus Rankin, *Chinese Local Elites and Patterns of Dominance* (Berkeley: University of California Press, 1990), 3; James Kai-sing Kung, and Chicheng Ma, "Friends with Benefits: How Political Connections Help Sustain Private Enterprise Growth in China," *Economica* 85, no. 337 (January 2018): 41-74, <https://doi.org/10.1111/ecca.12212>; Ting Chen, James Kai-Sing Kung, and Chicheng Ma, "Long Live Keju! The Persistent Effects of China's Imperial Examination System," *SSRN*, June 2017, <http://dx.doi.org/10.2139/ssrn.2793790>.

⁴⁶ Jonathan F. Schulz, Duman Bahrami-Rad, Jonathan P. Beauchamp, and Joseph Henrich, "The Church, Intensive Kinship, and Global Psychological Variation," *Science* 366, no. 6466 (2019): 5141, <https://doi.org/10.1126/science.aau5141>; Joseph Henrich, *The WEIRD People in the World: How the West Became Psychologically Peculiar and Particularly Prosperous* (New York: Farrar, Straus and Giroux, 2020), 196.

⁴⁷ Jonathan F. Schulz, "Kin Networks and Institutional Development," *SSRN*, September 1, 2016, <http://dx.doi.org/10.2139/ssrn.2877828>; Mahsa Akbari, Duman Bahrami-Rad, and Erik Kimbrough, "Kinship, Fractionalization and Corruption," *Journal of Economic Behavior & Organization* 166 (C) (2019): 493-528, <https://doi.org/10.1016/j.jebo.2019.07.015>.

⁴⁸ Hsiao-Tung Fei, "Peasantry and Gentry: An Interpretation of Chinese Social Structure and Its Changes," *American Journal of Sociology* 52, no. 1 (July 1946): 1-17, <https://www.jstor.org/stable/i328827>; Francis L. K. Hsu, *Under the Ancestors' Shadow: Chinese Culture and Personality* (New York: Columbia University Press, 1948); Maurice Freedman, *Lineage Organization in Southeastern China* (London: University of London and Athlone Press, 1958); Maurice Freedman, "Ancestor Worship: Two Aspects of the Chinese Case," in *Social Organization: Essays Presented to Raymond Firth*,

Yao⁴⁹ report that when one of the two largest family clans in a village is in charge, local public investment will increase, but at a price; the clans line their own pockets while colluding with local officials. Greif and Tabellini⁵⁰ show clan influence apparent not only in the resolution of civil and commercial disputes but also in the provision of welfare, securing property rights, protecting locals from official abuse, and even in contributions to public projects.⁵¹ Private firms today are mainly clan businesses, notes Zhang,⁵² who argues that “clan culture” is weakest in regions with a better market environment. Peng⁵³ records a strong and significant correlation of village-level kinship with the number of private enterprises, and Zhang, like Peng, suggests that this linkage contributes to the success of the pro-market reforms after 1979 by supplementing weak legal institutions. Foltz, Guo, and Yao⁵⁴ demonstrate that lineage connections help increase migration and public goods creation in fast-growing, newly populated areas. He, Pan, and Sarangi⁵⁵ report that lineage-homogenous villages are more likely to engage in

ed. Maurice Freedman (Chicago, IL: Aldine, 1967); James J. Watson, “Chinese Kinship Reconsidered: Anthropological Perspectives on Historical Research,” *The China Quarterly* 92 (December 1982): 589-622, <https://doi.org/10.1017/S0305741000000965>; Prasenjit Duara, *Culture, Power, and the State: Rural North China, 1900-1942* (Stanford: Stanford University Press, 1988); Myron L. Cohen, “Lineage Organization in North China,” *The Journal of Asian Studies* 49, no. 3 (1990): 509-34, <https://doi.org/10.2307/2057769>; Lily L. Tsai, “Solidary Groups, Informal Accountability, and Local Public Goods Provision in Rural China,” *American Political Science Review* 101, no. 2 (May 2007): 355-72, <https://doi.org/10.1017/S0003055407070153>.

⁴⁹ Yiqing Xu and Yang Yao, “Informal Institutions, Collective Action, and Public Investment in Rural China,” *American Political Science Review* 109, no. 2 (2015): 371-91, <https://doi.org/10.1017/S0003055415000155>.

⁵⁰ Greif and Tabellini, “The Clan and the Corporation.”

⁵¹ Relying on the China Social Survey, 2005 (Greif and Tabellini, “The Clan and the Corporation.”) calculate that “almost 70 percent of the population live in a county with positive sample probability of a village having a [clan] organization, and in 41 percent of the counties the village-probability of having a clan organization is at least 50 percent. The percentage of clans that held common property ranged from 21% to 28%.” Their assessment of the role of clans in Chinese history mirrors the one set out here: clans shape the evolution of Chinese social organization and render its culture quite different from that of Western countries.

⁵² Chuanchuan Zhang, “Clans, Entrepreneurship, and Development of the Private Sector in China,” *Journal of Comparative Economics* 48, no. 1 (March 2020): 100-123, <https://doi.org/10.1016/j.jce.2019.08.008>.

⁵³ Yusheng Peng, “Kinship Networks and Entrepreneurs in China’s Transitional Economy,” *American Journal of Sociology* 109, no. 5 (March 2004): 1045-74, <https://www.journals.uchicago.edu/doi/10.1086/382347>.

⁵⁴ Jeremy Foltz, Yunnan Guo, and Yang Yao, “Lineage Networks, Urban Migration and Income Inequality: Evidence from Rural China,” *Journal of Comparative Economics* 48, no. 2 (June 2020): 465-82, <https://doi.org/10.1016/j.jce.2020.03.003>.

⁵⁵ Quqiong He, Ying Pan, and Sudipta Sarangi, “Lineage-Based Heterogeneity and Cooperative Behavior in Rural China,” *Journal of Comparative Economics* 46, no. 1 (March 2018): 248-69, <https://doi.org/10.1016/j.jce.2017.10.006>.

reciprocal behavior with their lineage members and to contribute to the provision of public goods jointly shared across lineages than with people living in lineage-heterogeneous villages. Village-wide lineage groups are significantly correlated with the provision of public goods and with holding public officials accountable in Tsai.⁵⁶ Kinship-based organizations have survived reforms of the communist revolution. From 1949 to 1979, clans were officially disbanded, their property taken, their rules invalidated, and their genealogies burned. Yet once prohibitions were removed, their cultural sway over the social norms of the population resurfaced. All told, recent scholarship demonstrates that reliance on informal institutions of lineage groups solves collective action problems by facilitating the mobilization of local resources and the provisioning of local public goods – but at the risk of collusion and with a negligible impact on local government accountability. This replicates the patterns of ancient times.

The *Charities Aid Foundation* (CAF) World Giving Index⁵⁷ ranks China lowest of all 128 countries on willingness to help a stranger, donate money, or volunteer time. The CAF report describes how official decision-making does not meaningfully engage local communities. Civil society organizations are under strict surveillance, lack consistent regulation, rarely speak out independently on public issues, and garner only low levels of trust. All told, impersonal trust-building institutions in China, along with the codification of contractual relations, have lagged behind analogous European institutions by almost a millennium. Centola's approach suggests an answer to these examples of cultural persistence. Information can travel along long paths that span the system, but behavioral change requires bridge wideners that enable strong social reinforcement when significant personal investment is needed for adoption to occur.⁵⁸

Although kinship intensity is a characteristic that China shares with many other low-performing regimes, the weakness of civic bonds across communities did not prevent the emperors from ruling over the vast empire. In this regard, imperial China was not unlike the Roman and Ottoman empires and many other historical regimes operating with complex macro coordination while depending on lineage organization at the micro level. Yet its meritocratic and relatively inclusive civil service system is an attribute that has few parallels in world history or among developing nations today.

⁵⁶ Tsai, "Solidary Groups, Informal Accountability, and Local Public Goods Provision in Rural China."

⁵⁷ Charities Aid Foundation (CAF), "CAF World Giving Index: Ten Years of Giving Trends," Report, 10th Edition (London, UK: Charities Aid Foundation, October 2019), <https://www.cafonline.org/about-us/publications/2019-publications/caf-world-giving-index-10th-edition>.

⁵⁸ Damon Centola, *Change: How to Make Big Things Happen* (Little, Brown Spark, January 2021), 95-109.

State, Nation or Civilization: Cultural Sources of Chinese Longevity

How could two seemingly contradictory forces—the meritocratic civil service system and lineage and ancestor worship—operate in one system? These two conflicting characteristics of China’s development have long baffled scholars. Clearly, China’s extraordinary longevity cannot be credited to the long linkages of the political regime alone, as dynasties were shattered many times. I suggest that during periods of state decline and imperial collapse, the stability of the system derives from its hyperlocal networks and the lineage ordering of the grassroots society. They became a temporary system of “life support” that sustained the long-term continuity of Chinese culture. When the benefits of path-shortening infrastructure were undermined, communities depended on the most basic units of the society until the system-spanning order, the bureaucratic infrastructure, could be rebuilt. Although hyperlocal connectivity did not enable sustainable *system-spanning* connectivity, it did not allow imperial collapse to cause the death of Chinese culture. The idea of China as a civilization survived even as the state receded.

The different roles of voluntary civic associations have had another long-term effect in both regions: National identity among the populations of Western Europe is today expressed in terms of the Enlightenment – in the construction of individualism and law. In China, nationalism still finds expression in the heuristics of kinship and ancestor worship. Appeals to national unity are premised on ties of ethnic origin rather than a political choice or social contract, pitting its “humanism” against Europe’s.⁵⁹ Considering these tendencies that characterize Chinese ethical thinking, it is difficult to identify a Chinese philosophical tradition that would encourage a belief in a continual cultural advance towards a common law of human rights founded upon the principles of human nature and human reason.

Conclusion

In *Analyzing Social Networks*, Borgatti, Everett, and Johnson write: “Investigations into small-world and scale-free networks are usually confined to describing these properties, that is, deciding whether a network is a scale-free or small-world. The consequences of such structures are not well understood, and it would be difficult to draw conclusions about individual actors or even small groups of actors in such networks. The main goal is to gain some understanding of the overall network structure.”⁶⁰ This inquiry is a pioneering effort to apply

⁵⁹ Chinese Communist Party’s claims over Taiwan stress their same “blood” connection and it has launched an information campaign to overcome the marginal existence of the blood tie in Taiwanese national identity (*guojia rentong*). See Gang Lin and Weixu Wu, “Chinese National Identity under Reconstruction,” in *Taiwan and China: Fitful Embrace*, ed. Lowell Dittmer (Oakland: University of California Press, 2017), 75-92.

⁶⁰ Stephen P. Borgatti, Martin G. Everett, and Jeffrey C. Johnson, *Analyzing Social Networks*, 2nd ed. (London, UK: Sage Publications, 2017), 303.

models of the overall network structure to the circumstances and social organization of actual historical regimes and has uncovered patterns of relevance to network scientists, political economists, and scholars seeking to identify the fundamental characteristics of world civilizations. It has afforded new insights into recurrent, recognizable, and familiar patterns observed in historical political economy, such as the persistent trending of Chinese regimes toward authoritarian centralization. Why, in its transition to the impersonal complexity of a modern economy, does China still rely less on private markets and organizations and more on the state?⁶¹ What structural features support the persistently low levels of prosocial trust and high levels of *guanxi*, or relationship-based exchange?

China and the European West have social networks to solve problems such as information asymmetry in the economy. These can be sources of informal constraints that either discourage or boost cooperation and can hinder or build bonds and communities beyond kinship. The differences in how informal norms are disseminated and embedded in formal structures are recognizable with the help of network science. We have seen that during the urbanization of Europe's medieval period, the spread of voluntary civic associations increased the number of nodes in one community that had links to nodes in another, weakening lineage communities and homophily. Christian doctrine and institutions abetted this process. As community partitions were removed, connectivity increased across the system, producing a "metropolitan" ethos. In China, Confucian ethics reinforced partitions between homogenous communities with strong relational ties to lineage but weak moral obligations to other communities. This parochialism limited the spread of behavioral innovation between communities and instead created a "village" ethos in which relationship-based solutions preside over anonymous market exchanges.⁶² The emphasis on being centralized vs. decentralized is an insufficient framework to explain these patterns. My explanation for these longstanding differences with the West is that China had its own path shorteners—the system of mandarin bureaucracy with recruitment from across the empire—that enabled it to reach scale as a state and provided system-spanning connectivity but limited means to penetrate the parochial networks that enforced local norms.

My claim—that pattern of connectivity among the high-degree hubs fundamentally affects the system's robustness and that China's star-shaped topology is more vulnerable to major and immediate fragmentation if the center collapses—does not mean that China's leadership cannot overcome its deep-seated conservatism and aversion to cultural and technological transformation. On the

⁶¹ John Ray Bowen II and David C. Rose, "On the Absence of Privately Owned, Publicly Traded Corporations in China: The Kirby Puzzle," *The Journal of Asian Studies* 57, no. 2 (1998): 442-52, <https://doi.org/10.2307/2658832>.

⁶² Samuel Bowles and Herbert Gintis, "Persistent Parochialism: Trust and Exclusion in Ethnic Networks," *Journal of Economic Behavior & Organization* 55, no. 1 (September 2004): 1-23, <https://doi.org/10.1016/j.jebo.2003.06.005>.

contrary, the regime in Beijing is confident that it will maintain social order without constraining its mastery of the disruptive technologies of the future, nor does it recoil from the ethical implications of developing technologies that exploit the individual to benefit the collective. In fact, leadership would argue that the regime is pursuing the “higher ethical good.” In the West, the legacy of rights-granting norms shapes how the higher ethical good is defined. Differences in network topology provide both societies with differing capacities for monitoring and regulation, as well as durability and the ability to integrate new nodes and embody self-organization. With these insights derived from network science about connectedness, components, and the processes of change, researchers have a new approach to how cooperation scales in historical regimes and how cultural variations among populations form. They can now include network structure as an independent explanatory variable to the list of endogenous factors that sets world civilizations on different development trajectories.

Disclaimer

The views expressed are solely those of the author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium’s editors.

There are no conflicts of interest to disclose. There has not been any financial support provided for the conduct of the research and/or preparation of the article, nor provided for the writing of this article. This research did not involve Human Participants and/or Animals.

Data Availability

The data that support the findings of this study are available from the corresponding author upon request.

About the Author

Hilton L. Root is an American academic. He is a professor of public policy at the Schar School of Policy and Government of George Mason University in Virginia. He specializes in international political economy and international development. E-mail: hroot2@gmu.edu



Research Article

Security Aspects of Hybrid War, COVID-19 Pandemic and Cyber-Social Vulnerabilities

Chad Briggs,¹ Yuriy Danyk,² and Tamara Maliarchuk³

¹ *University of Alaska Anchorage, <https://www.uaa.alaska.edu>*

² *National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute," <https://kpi.ua/en/>*

³ *NATO DEEP Working Group, <https://deeportal.hq.nato.int/eacademy/>*

Abstract: While developments in cyber technologies have advanced the propagation and reach of hybrid warfare, the COVID-19 pandemic has accelerated many vulnerabilities and critical dependencies. This article explores the fundamental aims and strategies of hybrid warfare in terms of psychological underpinnings and technological reach and links to emerging issues of disinformation, cybercrime, fake news, information trauma, and the influence of new modes of education on national security and state resilience.

Keywords: hybrid warfare, cyberattack, cyber security, information trauma, e-learning, emotional warfare, cognitive hacking, cyber-social vulnerabilities, cyber technologies, COVID-19.

Introduction

The concept of hybrid warfare has gained increasing attention in security and military strategy discussions, often focused on examples of Russian operations in the takeover of the Crimean Peninsula of Ukraine in 2014. As a full-spectrum approach to understanding offensive operations, ranging from social media campaigns to conventional (kinetic) warfare, the term hybrid warfare can be used to describe a wide variety of activities. Most often, the emphasis is on the irregular nature of operations, where traditional, Western understandings of conflict are masked with forces and tactics that cannot easily be traced to a state adversary.

In our previous articles, we have detailed the use of cyber technologies in carrying out a broad range of attacks on Ukraine since 2013, including specific attacks on energy infrastructure.¹ In explaining countries' vulnerabilities to the loss of control over energy supplies, one key factor was the adversary's ability to undermine public trust in institutions, i.e., when basic needs are not met, social cleavages in a country or region are worsened, and governance becomes more difficult.

That hybrid wars are currently occurring worldwide is not disputed. Countries from Russia to China have incorporated ideas of fourth-generation warfare (4GW) into military doctrine for decades, where the "red line" between peace and war dissolves and adversaries are dealt with as part of an overall strategy of asymmetric, shadow (*maskirovka*) conflict.² These are not wars in the traditional sense of the Hague or Geneva Conventions, with clear starting and end points, of physical occupation of territory, and with visible actors and clear intent. Hybrid wars shift across borders and can maintain a quality of permanence, attacking entire countries at times while at other times focusing on specific groups or individuals. But hybrid war actions always have a goal and marshal the resources to achieve it. Everything else is just a tool to achieve this goal in the interests of particular players (actors). The critical component is a comprehensive strategy of one actor to keep the other off balance, destabilized enough that strategic space opens for political, economic, and military actions.³

Hybrid wars are a kind of permanent war of variable intensity across multiple sectors, with cascading, negative impacts, and synergistic effects, in which the entire population of the country and the international community are, to a certain extent, consciously or unconsciously involved. The impacts are felt in all spheres of life, in all sectors of society, and throughout the state. Thanks to the use of innovative technologies, it has become possible to shift conflict from predominantly overt and forceful (kinetic) means to less obvious strategies focused on the structural vulnerabilities of adversaries, including by achieving cognitive advantage and control over them.

Such hybrid tactics make it possible to take control of or destabilize the basic institutions of a country and achieve strategic interests via unconventional cyber and cognitive influences (including spillover effects). Cyberspace has proven to be the main theater of asymmetric actions. It is supported by the fact that cyberspace has an extraterritorial, universal, and global character. It is also ill-adapted to national geographic borders, can serve as socializing surroundings for

¹ Yuriy Danyk, Tamara Maliarchuk, and Chad Briggs, "Hybrid War: High-tech, Information and Cyber Conflicts," *Connections: The Quarterly Journal* 16, no. 2 (2017): 5-24, <https://doi.org/10.11610/Connections.16.2.01>.

² Robert Wilkie, "Hybrid Warfare: Something Old, Not Something New," *Air & Space Power Journal* 23, no. 4 (Winter 2009): 13-18.

³ Daniel T. Lasica, *Strategic Implications of Hybrid War: A Theory of Victory* (FT Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies, 2009), <https://apps.dtic.mil/sti/pdfs/ADA513663.pdf>.

people of nearly all ages, and is constantly expanding in scope and influence. Information flows can be realized through dialogue with mass audiences while at the same time using social media to achieve or mimic individual communication. For the time being, cyber technologies prove to be the most important instrument for shaping collective and individual consciousness and social values.

Cyber technologies, therefore, allow for hybrid strategies to realize goals of widespread impacts on society at a distance and without clear attribution to the aggressor. The most effective users of cyber-hybrid approaches determine the end effects to be realized and marshal an appropriate array of synergistic actions with overlapping, cascading, and reinforcing impacts. These impacts are focused on disabling an adversary, promoting prearranged narratives, and controlling the cognitive sphere on the emotional, moral, cultural, and mental levels. Successful actions can create a system of stable stereotypes and the perception of reality or merely foster instability and the denial of objective standards and truth.

The COVID-19 pandemic, which has ravaged the planet since December 2019, added its own peculiarities to the spectrum of hybrid confrontations and methods. It must be considered when analyzing them and making forecasts to reduce their risks and prevent and/or mitigate their consequences. This article focuses on the social nature of hybrid warfare and how technologies allow for the exploitation of social and political vulnerabilities and polarization in target states. These issues were also examined in the context of hybrid warfare, the COVID-19 pandemic, and emerging cyber-social vulnerabilities.

While attention to the military and physical infrastructure of hybrid attacks remains important, such offensive operations rely upon fragile social and political fabrics that remain integral to planning offensive strategies and appropriate defense against hybrid attacks. Historical experience has shown that hybrid warfare actions in this sphere favor the attacker – while countries such as the United States have used hybrid methods in the past to shore up political support in conflict areas, success (e.g., 1950s Philippines) is less common than failure (post-2003 Iraq or Afghanistan).⁴ Particularly where an aggressor has detailed knowledge of one's opponent, social divisions are easy to exploit and have become much more vulnerable with the skillful use of cyber tools such as social media. Using examples from Ukraine and the United States, this article details ways in which technology is leveraged as an asymmetric approach to influencing and undermining an adversary's governance.

The idea of attacking the social fabric of one's adversary is hardly new. Sun-Tzu advocated attacking the morale of one's adversary and warned that protracted conflict would lower public support for wars.⁵ Clausewitz likewise identified the political nature of warfare, understanding that winning a conventional

⁴ Ivan Arreguin-Toft, "How to Lose a War on Terror: A Comparative Analysis of a Counterinsurgency Success and Failure," in *Understanding Victory and Defeat in Contemporary War*, ed. Jan Angstrom and Isabelle Duyvesteyn (Routledge, 2006), 160-185.

⁵ Sun Tzu, "The Art of War," in *Strategic Studies: A Reader*, ed. Thomas G. Mahnken and Joseph A. Maiolo (Routledge, 2014), 86-110.

battle may not be sufficient for winning the wider war.⁶ Counterinsurgency and irregular warfare experts through the 20th century were even clearer in emphasizing the importance of public morale off the traditional battlefield and pointing out that direct military force can prove to be counter-productive in winning political support in a conflict. US Air Force debates over the use of strategic bombing have been a case in point, particularly its use against civilian targets during the Second World War in Europe. While officially targeting industrial or military targets, the US approach to high-altitude bombing in Europe often resulted in high civilian casualties, with an argument (made more forcefully by the Royal Air Force) that the destruction of cities would undermine public morale and support for German aggression against the West.⁷ The German Luftwaffe made similar arguments for their bombing campaign against the UK in 1940-41 and with similarly disappointing results.⁸ Rather than German or British morale breaking by seeing their cities destroyed and neighbors killed by aerial bombing, the public tended to rally around their state in response to such open aggression.

Similarly, decades later, US military actions against Vietnamese villages suspected of harboring Viet Cong (VC) insurgents only seemed to increase support for the VC or at least direct public opinion against the Americans.⁹ Carr argued that open violence against civilians (as opposed to the military), whether by the US military in Vietnam or the Irish Republican Army in the UK/Ireland, led to perceptions of illegitimate actions and loss of popular support among the population.¹⁰ Yet the key ingredient in such assessments was the visibility of such actions and their clear intent. In cases where aggressive actions could be blamed on others (false flag attacks) or where the nature of the attack fell below physical violence, attribution and blame tended to fall apart.

A House Divided

The Russian military approach to warfare has long recognized the need for asymmetric approaches to conflict, meaning where an adversary's vulnerabilities would be used against it, disproportionate to the amount of force available. A common approach for Russian activities is to use influence operations, activities

⁶ Carl von Clausewitz, *On War* (Penguin UK, 1982).

⁷ Kenneth P. Werrell, "The Strategic Bombing of Germany in World War II: Costs and Accomplishments," *The Journal of American History* 73, no. 3 (December 1986): 702-713, <https://doi.org/10.2307/1902984>.

⁸ Edgar Jones, Robin Woolven, Bill Durodié, and Simon Wessely, "Civilian Morale During the Second World War: Responses to Air Raids Re-examined," *Social History of Medicine* 17, no. 3 (2004): 463-479, <https://doi.org/10.1093/shm/17.3.463>.

⁹ Richard Shultz, "Breaking the Will of the Enemy During the Vietnam War: The Operationalization of the Cost-Benefit Model of Counterinsurgency Warfare," *Journal of Peace Research* 15, no. 2 (June 1978): 109-129, <https://doi.org/10.1177/002234337801500202>.

¹⁰ Caleb Carr, *The Lessons of Terror: A History of Warfare Against Civilians* (New York: Random House, 2003).

that fall below the threshold of most military responses in Western countries and can often be masked without the aggressor admitting its activities or intentions. Influence operations are intended to use largely indirect and non-kinetic means to sow discord and division within one's adversary, relying upon pre-existing ingroup/outgroup formations to polarize politics, delegitimize the government and its institutions, and target the resilience of its population and communities to respond to outside threats.¹¹ While the history of influence operations is not new, cyber technologies have allowed remarkable penetration from anywhere in the world straight to individuals' computers and phones, all while masking the true source of information and disinformation.

In some military strategies, including those of the Russian Federation and China, there is a marked focus on information operations as part of larger strategies and operations, not separated as they often are in the US and Western Europe. Whether this is referred to as part of the "Revolution in Military Affairs" or other doctrines, in practical terms, these strategies refer to asymmetric and information-focused active measures against an opponent. As detailed by the US State Department in 1989 in reference to Soviet activities, "active measures" referred to a combination of disinformation and forgeries, front groups, non-ruling opposition parties, and political influence operations. Taken together, these were the basis for *maskirovka*, or the masking of warfare in the guise of harmless acts.¹²

As Bagge described the concept of reflexive control in the Russian strategy, "Reflexive control serves to undermine the very decision-making system itself, to make it favorable to the projector and thus to project power without committing significant military or political resources, nor meeting the acknowledged threshold of meddling in a sovereign's international affairs."¹³ Reflexive control was a development of Soviet military doctrine that emphasized both disruption of the enemy's decision-making processes and feeding of disinformation in such a way that the enemy would react in a way advantageous to the Soviets/Russians. If an enemy commander perceived that his choices were limited to certain options, successful reflexive control would occur when those options played into Russian strategy, and the decision would be easier to anticipate.

Taken together, hybrid warfare, as understood by the Russian government and military, envisions a coherent strategy to undermine and destabilize an adversary, using a broad spectrum of means but (when possible) using an enemy's own weaknesses to play into the Russian strategy. The concept of reflexive control, after all, was to influence the information available to military officers, leading them into a predetermined (by the Russians) course of action that could be

¹¹ Maria Snegovaya, "Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare," Russia Report 1 (Washington DC: Institute for the Study of War, September 2015).

¹² Daniel P. Bagge, *Unmasking Maskirovka: Russia's Cyber Influence Operations* (Washington, DC: Defense Press, February 2019).

¹³ Bagge, *Unmasking Maskirovka*.

planned for and which would play to Russian strengths in the battlespace. While difficult to realize fully in traditional warfare (although the British military and intelligence services have historically been more successful than many at strategic misdirection), with cyber technologies, the ability to achieve disinformation can be heightened. When successful, not only is the targeted society increasingly fragmented, but the targets themselves become messengers of disinformation and negative narratives.

Cognitive Hacking

Taking advantage of new and more widespread technologies, attackers are increasingly using psychological tricks and manipulations in the cognitive space. These tactics often mirror those used by hackers (phishing, spoofing, and others) and are a particular type of social engineering. Their use increases the possibility of gaining unauthorized access to information resources in cyberspace that are critical for the cognitive sphere of society, with the possibility of destructive effects on them. This phenomenon is called “cognitive hacking.”¹⁴ It is based on the manipulation of public consciousness performed in cyberspace – not only to steal money or data but also to influence the behavior of users, impose their will on them and control them. Almost any user of cyberspace can use cognitive hacking through disinformation campaigns and manipulation of reputation and/or distribution on Internet platforms of content that changes the perception of reality among other users. It can be carried out in the form of cyberattacks, cyber actions and operations aimed at manipulating the human perception of reality using the vulnerabilities of how people and social media process information. Such attacks aim to alter human behavior, perception, or attitude toward significant events or topics like the COVID-19 pandemic and are tailored toward a specific goal.¹⁵

In 2019 the volume of phishing attacks (the creation of fake sites or links that mimic the sites of well-known companies) grew by 400%. At the same time, more than 24% of malicious page addresses (URLs) were located on legitimate domains, relying on users’ trust in them, and phishing became more personalized, including tracking the presence and activities of a particular user in cyberspace.¹⁶ In addition to phishing, cybercriminals also use spoofing (disguising a

¹⁴ Darren L. Linvill et al. “‘The Russians Are Hacking My Brain!’ Investigating Russia’s Internet Research Agency Twitter Tactics During the 2016 United States Presidential Campaign,” *Computers in Human Behavior* 99 (October 2019): 292-300, <https://doi.org/10.1016/j.chb.2019.05.027>.

¹⁵ Ian Baxter, “The Cognitive Psychological Tricks Hackers Use to Dupe Users,” *ITProPortal*, March 12, 2020, www.itproportal.com/features/the-cognitive-psychological-tricks-hackers-use-to-dupe-users.

¹⁶ Muhammad Adil, Rahim Khan, and M. Ahmad Nawaz Ul Ghani, “Preventive Techniques of Phishing Attacks in Networks,” in *Proceedings of the 3rd International Conference on Advancements in Computational Sciences*, ICACS 2020, Lahore, Pakistan, February 17-19, 2020 (IEEE, 2020), 1-8, ISBN 978-1-7281-4235-7.

malicious program as legal) as an in-road to political attacks. For example, in March 2016, one of the high-ranking officials of Hillary Clinton's campaign headquarters, John Podesta, entered his credentials on a page without recognizing a fake notification allegedly received from Google. After that, a hack occurred, and the attackers gained access to his data, which international and national political actors later exploited.¹⁷

Emotional Warfare

Along the murkier, non-kinetic spectrum of hybrid warfare, control of information targets not just cognitive processes but more limbic and emotional centers of the brain.¹⁸ Humans naturally divide the world into various categories of identity as a way of making sense of a complex world and explaining why things happen as they do. Political psychologists have long demonstrated that these categories need not possess any intrinsic value. They can be completely arbitrary, constructed from myths, or handed down from authorities, whether by dividing schoolchildren into random groups according to eye color or national categories based upon historical events from centuries earlier. To outsiders, such divisions may appear arbitrary, such as Jonathan Swift's satire of differences between Catholics and Protestants in 1723. Still, inside social networks, such divisions can appear real and be reinforced by political, economic, and media practices.

Psychologists have identified trajectories along which ingroup/outgroup divisions can be turned from socially acceptable differences to potentially violent and intractable antagonisms. First, differences are essentialized or naturalized, meaning that broad stereotypes are placed on a group explaining that social differences (whether racial, linguistic, religious, etc.) are essential features of the group being described. When one is born into or raised in such a group, these differences are considered solidified and cannot easily be changed. The outgroup is then devalued according to these traits, with media images and stories often constructed to amplify these negative stereotypes.¹⁹ These first two processes can often serve to help raise opinions of one's own group by highlighting differences in what makes one "good." American patriotism throughout the Cold War was often based on drawing the distinction between "hard-working Americans" and "inefficient, godless communists." In contrast, other nationalisms would

¹⁷ Travis Farral, "Nation-state Attacks: Practical Defences against Advanced Adversaries," *Network Security* 2017, no. 9 (September 2017): 5-7, [https://doi.org/10.1016/S1353-4858\(17\)30111-3](https://doi.org/10.1016/S1353-4858(17)30111-3).

¹⁸ Linton Wells II, "Cognitive-Emotional Conflict: Adversary Will and Social Resilience," *Prism* 7, no. 2 (December 2017): 4-17, <https://cco.ndu.edu/PRISM-7-2/Article/1401814/cognitive-emotional-conflict-adversary-will-and-social-resilience>. We also credit Aleksandra Nestic for her work on emotional warfare.

¹⁹ Marilyn B. Brewer, "The Psychology of Prejudice: Ingroup Love and Outgroup Hate?" *Journal of Social Issues* 55, no. 3 (Fall 1999): 429-444, <https://doi.org/10.1111/0022-4537.00126>.

strive to highlight the achievements of their own culture above others.²⁰

The more dangerous progression is when the needs of communities are not or cannot be met, whether from basic needs, such as food becoming too expensive, to more existential threats of loss of culture or prestige. When such fears are present in a society, whether openly or latently, space opens for attribution of such threats to outsider groups. Historical anti-Semitism was often based on Jews being blamed for the financial troubles of the majority population, based upon stereotypes of their historical, social roles as bankers, lawyers, and academics. Dehumanization and/or depoliticization of groups, coupled with blame for a society's inability to reach basic goals or needs, draws upon perceived essential characteristics of a group to polarize opinion and accept violent remedies against the threatening outgroup.²¹

Propaganda campaigns during wartime have often employed such strategies, whether First World War stereotypes of German "Huns" killing innocent women and children, to US campaigns against the perceived fanaticism and inhuman nature of the Japanese.²² The starkest examples, of course, occurred when the dehumanization of a group took on such proportions that genocidal violence was accepted and encouraged, whether against Jews in the Second World War, Muslims in Bosnia-Herzegovina, or "undesirables" in Khmer-Rouge era Cambodia.²³ Yet open warfare and a progression toward genocide need not be present for social divisions to be critical nodes in a conflict. The hybrid war model stops short of sweeping violence against a population in favor of using an adversary's divisions against itself.

US-know Thyself

The United States intelligence community has raised warnings about Russian interference in the American political system since at least 2016. The recent Mueller Report indicated that serious Russian efforts to influence elections date back to no later than 2014. Rather than being what some critics dismissively refer

²⁰ Robert T. Schatz, Ervin Staub, and Howard Lavine, "On the Varieties of National Attachment: Blind Versus Constructive Patriotism," *Political Psychology* 20, no. 1 (March 1999): 151-174, <https://doi.org/10.1111/0162-895X.00140>. It should be noted that some nationalisms are negative in nature, focusing on historical defeats and a sense of victimhood.

²¹ Ervin Staub, "The Roots of Evil: Social Conditions, Culture, Personality, and Basic Human Needs," *Personality and Social Psychology Review* 3, no. 3 (1999): 179-192, https://doi.org/10.1207/s15327957pspr0303_2.

²² Harold D. Lasswell, *Propaganda Technique in the World War* (Ravenio Books, November 2015).

²³ Michał Bilewicz and Johanna Ray Vollhardt, "Evil Transformations: Social-Psychological Processes Underlying Genocide and Mass Killing," *Social Psychology of Social Problems: The Intergroup Context*, ed. Agnieszka Golec de Zavala and Aleksandra Cichońska (New York, NY: Palgrave Macmillan, 2012): 280, https://doi.org/10.1007/978-1-137-27222-5_11.

to as “a few Facebook ads,” the Russian efforts (both cyber and human) constituted a coordinated campaign to undermine trust in US institutions and increase political uncertainties and polarization.²⁴ That no definitive judgment has been made concerning precisely what effect such actions had on the 2016 elections is beside the point – if the goal was to increase uncertainty and undermine trust, even asking such questions has already accomplished a basic goal.

In many ways, the US was and remains a vulnerable target for cyber actions of hybrid warfare, even before the events of January 6, 2021. It is a country with deep political, economic, regional, racial, and gender differences. Most American political leaders have not emphasized the differences except along party lines, choosing instead to highlight common American political aspirations. Yet the latent differences and grievances remained available for exploitation, and cyber tools such as social media allowed unfettered access to millions of Americans. Led by the Russian GRU and IRA (Internet Research Agency), a directed campaign aimed to polarize Americans with such “wedge” issues as immigration, gender rights, and religion. A declassified US intelligence report from January 2017 summarized, “We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election. Russia’s goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess Putin, and the Russian Government developed a clear preference for President-elect Trump. We have high confidence in these judgments.”²⁵

The common perception was that, with Clinton as a front-runner in the election, Russian actions could help undermine her future presidency by sowing doubt as to its legitimacy. Cyber actions undertaken included infiltration of party (both Democratic and Republic) e-mail records, repackaging as cyber aggression selected communication via outlets like Wikileaks, creation of “astroturf” political groups on social media sites, sock-puppeting on sites like Facebook and Twitter to impersonate US voters, creation of fake protests and counter-protests, creation and dissemination of fake and misleading news reports, and much of this done through microtargeting selected populations in key states. The use of metadata from social media sites made this relatively easy, where users expressing keywords suggesting unease at immigration by Muslims, for example, could be fed ads and political messages to amplify such fears vis-à-vis certain candidates.²⁶

²⁴ Robert S. Mueller, “Report on the Investigation into Russian Interference in the 2016 Presidential Election,” The Final Report of the Special Counsel into Donald Trump, Russia, and Collusion (Washington, D.C.: US Department of Justice, March 2019), <https://www.justice.gov/archives/sco/file/1373816/download>.

²⁵ Bill Priestap, “Assessing Russian Activities and Intentions in Recent US Elections,” Unclassified Intelligence Community Assessment (Office of the Director of National Intelligence, January 2017), p. ii.

²⁶ Philip N. Howard et al., “The IRA, Social Media and Political Polarization in the United States, 2012-2018” (University of Oxford, 2018).

While these Russian tactics were often successful, they could only find traction in a political landscape where significant divisions already existed, where fake news and conspiracy theories could take hold in a significant proportion of the population, and where technology had sufficient penetration – at least 30 million Americans were exposed to Russian messaging.²⁷ Rather than see themselves as Americans fighting in common against Russian operations, people in the US turned on each other along divisions of ingroup and outgroup, using language referring to “our” people, “real” Americans, and references to loyalty. Moreover, the IRA did not limit itself to electoral politics. It was also active in anti-science campaigns, notably in climate change and anti-vaccination circles. That this has helped in spreading otherwise dormant diseases such as measles (by spring 2019, some US states had declared states of emergency for the outbreaks) cannot be attributed solely to Russian activity but was meant to inflame undercurrents already present in American society²⁸ like cyber-surfing on existing topics that are “sensitive” to society or individual target groups.

The COVID-19 pandemic highlighted many of these differences, with divisions being exploited or created in response to public health responses. Protests against COVID vaccines in 2021 included both left- and right-wing groups, with the use of masks to prevent the spread of the coronavirus being associated along party lines.²⁹ Many actors were eager to fan such fires, disputing the virus’s origins and its deadly nature, and such tropes were wrapped up in different disputes, more often politics than medicine. The larger strategy of both Russia and China was to cast doubt on the effectiveness of democratic institutions in response to the pandemic.³⁰

The political psychology of ingroup/outgroup divisions helps explain how, when these divisions were reinforced through media and political narratives, the divisions became much starker both to outside observers and those who identified with one camp or another. This has not only made traditional bipartisan legislation and governing extremely difficult at the federal level, but the divisions have intensified. When new disinformation is spread (or biased targeted content triggers predetermined (planned) processes or perceptions), whatever the original source, Americans can share such information from person to person via so-

²⁷ Howard et al., “The IRA, Social Media and Political Polarization.”

²⁸ David A. Broniatowski et al., “Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate,” *American Journal of Public Health* 108, no. 10 (October 2018): 1378-1384, <https://doi.org/10.2105/AJPH.2018.304567>; Shanta Barley, “Climategate: Russian Secret Service Blamed for Hack,” *New Scientist* 7 (2009).

²⁹ Rose Bernard, Gemma Bowsher, Richard Sullivan, and Fawzia Gibson-Fall, “Disinformation and Epidemics: Anticipating the Next Phase of Biowarfare,” *Health Security* 19, no. 1 (2021): 3-12, <https://doi.org/10.1089/hs.2020.0038>.

³⁰ Sergey Sukhankin, “COVID-19 as a Tool of Information Confrontation: Russia’s Approach,” *The School of Public Policy Publications* 13, no. 3 (April 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3566689.

cial media, with selection algorithms (such as with Facebook) further strengthening the perception that such information can be trusted, because a trusted fellow American shared it. While Soviet propaganda in the 1970s and 80s had to work very deliberately to launder sources via multiple fronts, with cyber tools, a message or narrative can be released and spread with little effort, provided it reflects what people want or expect to see.

Social media techniques do not stand alone. Effective hybrid warfare uses various tools to achieve the aim of disruption or control. Attacks on energy infrastructure have also been documented in the US, with the US government admitting that denial-of-service attacks had disrupted grid operations in the Western United States in March 2019. Following knowledge that such attacks were possible and that breaches had previously been attempted, this opens the real possibility that the US could be hit with disruptions of critical services similar to what had previously been witnessed in Ukraine (which, in a sense, has become a testing ground for the technologies of future wars, in particular cyber, informational, and cognitive actions). The strategic goal of such threats or actions would be to create a feeling of uncertainty and insecurity, to keep both citizens and decision-makers off-center and anxious about how to interpret events and information.

Events in the US are admittedly of a much lower step of escalation than in other countries (i.e., Georgia, Estonia, Ukraine, Syria). Still, it is important to reiterate that there is no “red line” that distinguishes hybrid war strategies in one country versus another. The goals vary in the degree of destabilization desired, with some consideration for what might trigger an active response to the aggressor state. What the US experience has shown is that incremental and covert actions can weaken the response threshold over time, allowing greater interference and destabilization without a strong and coordinated defense.³¹

It’s Warmer in the East

The continuing conflict in Ukraine is often cited as one of the primary examples of hybrid warfare in recent years, although many analyses refer primarily to the occupation of Crimea in 2014. The open conflict in regions of Donetsk and Luhansk since mid-2014 has received less attention and is often erroneously referred to in the western media as a “civil war.” Even when analyses include discussion of violent conflict in the east, including the downing of Malaysian Airlines flight MH-17 in July 2014, these violent actions represent only the most visible aspects of the hybrid warfare spectrum.³² This conflict has a number of specific

³¹ Rubén Arcos, Manuel Gertrudix, Cristina Arribas, and Monica Cardarilli, “Responses to Digital Disinformation as Part of Hybrid Threats: A Systematic Review on the Effects of Disinformation and the Effectiveness of Fact-checking/Debunking,” *Open Research Europe* 2, no. 8 (2022), <https://doi.org/10.12688/openreseurope.14088.1>.

³² Irina Khaldarova and Mervi Pantti, “Fake News: The Narrative Battle over the Ukrainian Conflict,” *Journalism Practice* 10, no. 7 (2016): 891-901, <https://doi.org/10.1080/17512786.2016.1163237>.

features, the most notable of which is the emerging evidence of non-kinetic (i.e., information warfare) having significant trauma impacts within society far from the front lines of eastern Ukraine.

Destructive actions focus on critical nodes in social and related systems, vulnerabilities that can be exploited, and then take on a self-sustaining, downward cycle of repeated steps and impacts (in scientific terms, positive feedback loops). Yet as the targeted nodes are dispersed across geographical and functional areas, it can be difficult for an outside observer to see the pattern of intended impacts and the overall strategy of the aggressor. It is vital for national security strategies to be able to identify and resist such dispersed and covert actions and to understand the complex and cascading impacts of aggressive actions that do not trigger the traditional concept of “acts of war.”

As with other complex security systems, such as energy and environment, it is often not the initial impact that is most critical but the second and third-order effects that stem from the original disruption. Causal chains of events can be difficult to see at first, and inappropriate responses can worsen the chains of impact.³³ For instance, the Soviet government’s response to the 1986 Chernobyl nuclear power disaster stands as perhaps one of the worst examples of a response. Then, political considerations led to the radiation exposure of tens of thousands of citizens in Ukraine and beyond. Similarly, inappropriate responses to changing conditions can easily worsen other disasters or conflicts.³⁴ Following precepts of reflexive control, an effective hybrid warfare campaign can lead a government into a positive feedback loop of worsening second and third-order impacts.

The hybrid war undertaken in Ukraine exhibits these strategic considerations of coordinated and planned actions and contains the necessary components in the cyber domain:

- Overall goals to be achieved
- Strategy for undertaking the campaign
- Organization of the campaign
- Tactics and instruments to be used
- Primary, secondary, and tertiary impact assessment
- Evaluation and reinforcement of consequences.

Cyber actions can be carried out sequentially, simultaneously, in parallel, and both in dispersed and focused manners. Dispersed-focused cyber actions aim at the infrastructure’s most vulnerable elements (objects). A set of simultaneous and/or sequential cyber impacts provides synergistic effects on unpredictable

³³ Aura Reggiani, “Network Resilience for Transport Security: Some Methodological Considerations,” *Transport Policy* 28, no. C (2013): 63-68, <https://doi.org/10.1016/j.jtrapol.2012.09.007>.

³⁴ Andrew Leatherbarrow, *Chernobyl 01:23:40: The Incredible True Story of the World’s Worst Nuclear Disaster* (Lancaster, UK: Andrew Leatherbarrow, 2016).

places (elements, systems, spheres) that may be administratively or politically separated from the initial target but functionally influence critical systems. As an example from the non-cyber world, in 2001, a series of anthrax attacks occurred on politicians via the US postal system, which was then forced to shut down mail rooms across Washington D.C. An unanticipated (for disaster planners) impact was that payment checks to the local utility PEPCO were not received, and the electrical utility had to approach the White House asking for funding, lest it cut off power to the US capital.³⁵ Cyber actions can have more immediate consequences in an even more interconnected world where companies rely on electronic payments and just-in-time deliveries of goods and components. For example, the June 2017 Petya cyberattacks on Ukraine had spillover effects into the European and global financial systems, even though the primary target was the Ukrainian state and domestic companies on the eve of the national holiday.³⁶

While the 2017 Petya attacks met with an effective response from Ukrainian cyber forces, the intended targets of financial institutions quickly spilled over into hospitals and insurance companies around the globe. These methods work by designing cyber impacts with widespread chain effects. They disperse a destructive wave on interrelated objects and systems, simultaneously sparking impacts on multiple overlapping spheres. Cyberattacks can be implemented synchronously or asynchronously, in parallel along several lines of attack, or in serial multiple times on the same target cluster. Damage to the target objects is most destructive and effective according to the criteria of “efficiency-time-cost,” although some targets may serve as a proof-of-concept to demonstrate capabilities to other potential target countries. A combination of research and combat analyses indicates that cyber-related actions and information warfare are increasing in scope and importance for warfighters.³⁷ In this context, hybrid warfare and its use of cyber assets are among the most important factors for understanding the future arc of conflict.

The December 2015 Russian cyberattack on the Prykarpattya Oblenergo power station required months of careful preparation and infiltration but disrupted electricity delivery for less than a day. It is possible that the real target of the attack was not just Ukraine. The attack might have been a test of new hybrid warfare techniques and a warning to other countries whose energy systems may be vulnerable to similar tactics. New cyberattacks in 2021 and early 2022 confirm

³⁵ Reshma Pradhan Lensing, “Historical Events and Supply Chain Disruption: Chemical, Biological, Radiological and Cyber Events,” PhD Dissertation (Massachusetts Institute of Technology, 2003).

³⁶ Jagmeet S. Aidan, Harsh K. Verma, and Lalit K. Awasthi, “Comprehensive Survey on Petya Ransomware Attack,” In *Proceedings of the 2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS)*, IEEE, pp. 122-125.

³⁷ Iskren Ivanov and Velizar Shalamanov, “NATO and Partner Countries Cooperation in Countering Asymmetric and Hybrid Threats in South Eastern Europe’s Cyberspace,” in *Toward Effective Cyber Defense in Accordance with the Rules of Law* 149, ed. Alan Brill, Kristina Misheva, and Metodi Hadji-Janev (2020): 59-70, <https://doi.org/10.3233/NHS DP200041>.

that a real information and cyber war is being waged on Ukraine, including the entire range of destructive impacts on both technical infrastructure and society. The use of social media to carry out cyberattacks is even more cost-effective, as they take advantage of the systems' own algorithms to spread disinformation or targeted narratives. Millions of people can be reached with relatively little effort, and when coupled with cyberattacks elsewhere (institutions, infrastructure), the social impacts can be sharply heightened.³⁸

A Hybrid Form of Collective Trauma

The chaotic background of not knowing the future security risks in a country, how to interpret information or who to trust, and whether one can rely upon essential services or institutions, amplified by hybrid warfare, can lead to widespread states of cognitive resonance, dissonance, or imbalance. Beyond the confusion described by cognitive psychology, people can receive injuries measurable in terms of biological and neurological pathologies, where both individual and collective psychologies are pushed beyond normal perception, interpretation, and trust and fall into varying degrees of trauma.³⁹ Studies in Ukraine have measured the effects of trauma in zones near open conflict in the east. More recent research indicates that a more significant "hybrid war syndrome" may exist when the entire territory is a zone of active, destructive impacts upon individual and social psychologies.

The hybrid war consequences are not limited to the number of dead, maimed, and missing. They also include the effects on the cognitive sphere of citizens, communities, and society as a whole. Hybrid warfare, directly and indirectly, influences the conscious and subconscious, psychophysiological, mental state, and public health of conflict participants and bystanders. But in the cyber world of a hybrid conflict, witnesses do not only exist in the "hot zones" of kinetic warfare. Entire populations witness the conflict and are actively targeted by campaigns to undermine traditional concepts of identity, trust, and objective reality. In previous conflicts, trauma was experienced by those in a geographically defined war zone or where media could transmit disquieting images of war into people's living rooms. In contrast, cyber tools allow greater reach, erasing the older geospatial boundaries and one-way information flow. Both combatants and civilians, therefore, find themselves in the hybrid conflict zone, which manifests a number of psychological and behavioral characteristics that can be collectively labeled as "hybrid war syndrome" and its derivatives, "military-specific hybrid war syndrome," "specific PTSD of hybrid warfare," and others.⁴⁰

³⁸ Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, March 3, 2016, www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid.

³⁹ Jack Saul, *Collective Trauma, Collective Healing: Promoting Community Resilience in the Aftermath of Disaster* 48 (Routledge, 2013).

⁴⁰ Yuriy Danyk and Oleksandra Zborovska, "Development and Implementation of a New Concept of Crisis Situations Syndrome: 'Syndrome of a Hybrid War'," *EUREKA: Health*

In countries experiencing protracted conflict, a stratum of people has developed a “military-specific hybrid war syndrome.” This syndrome is attributed to the low, direct combat (military/kinetic) intensity of hybrid conflicts and the wide spectrum of unconventional parallel actions. Those experiencing heightened exposure to violence in a conflict zone often undergo substantial changes to individual psychology and reactions to the society around them, particularly when they return from the conflict zone and experience serious cognitive dissonance and dissociation.⁴¹ Such individuals may have combat skills not applicable in civilian life and experience *hyperarousal* of threat perceptions (including potential aggression against imaginary threats), *intrusion* of traumatic memories on all aspects of life, and *constriction* in feeling that the traumatic experiences cannot be escaped. What differentiates this form from traditional combat trauma is that returning soldiers or participants do not return to a condition of peace or stability. Instead, they are still operating in an unstable environment in which threats and triggers permeate daily life.⁴²

In many ways, the strategies of hybrid warfare not only create situations of direct trauma but mimic dissociative conditions for so long that psychobiological responses are indistinguishable. In describing combat trauma, Kardiner wrote, “...the whole apparatus for concerted, coordinated, and purposeful activity is smashed. The perceptions become inaccurate and pervaded with terror, the coordinative functions of judgment and discrimination fail... the sense organs may even cease to function.”⁴³ In a hybrid war environment, an individual attempting to cope with constant stress and feelings of threat, hopelessness, and loss of control cannot easily rely on larger social reserves of resilience. When social trauma is experienced and groups begin to fragment, uncertainty and perceptions of risk are amplified by fellow members of society, a phenomenon greatly enhanced by accessing and using social media.

Those not experiencing combat or violence at the “front lines can still experience many of the stressors related to PTSD, and prolonged exposure to these influences has been shown to manifest as biophysiological markers in medical studies.⁴⁴ Though perhaps not surprising given hybrid war methods, it is remarkable that cyber tools allow penetration of acute stress into areas far removed

Sciences 6 (2018): 15-29, <https://doi.org/10.21303/2504-5679.2018.00797>; Piotr Pacek and Olaf Truszczyński, “Hybrid War and Its Psychological Consequences,” *Torun International Studies* 1, no. 13 (2020): 23-30, <https://doi.org/10.12775/TIS.2020.002>.

⁴¹ Yuriy Danyk et al., “The Technology of Objective Diagnosis, Treatment and Prevention of PTSD in Members of the Armed Forces under Conditions of Hybrid War,” *International Journal of Research and Innovation in Applied Science* 4, no. 1 (January 2019): 7-11, www.rsisinternational.org/journals/ijrias/DigitalLibrary/Vol.4&Issue1/07-11.pdf.

⁴² Judith L. Herman, *Trauma and Recovery: The Aftermath of Violence – From Domestic Abuse to Political Terror* (New York: Basic Books, July 2015).

⁴³ As quoted in Herman, *Trauma and Recovery*, 35.

⁴⁴ Iryna Boichuk et al., “Characteristics of Eye Movements in the Anti-terrorist Operation Area’s Residents with Potential Posttraumatic Stress Disorder,” *Journal of Ophthalmology* 1 (Ukraine) (2019): 52-55; Yuriy Danyk et al., “The Objectivization of the Complex

geographically from traditional conflict. These syndromes appear as a consequence of long-term, collective, and individual trauma from threats to life and health, to the constant change of form and intensity of combat tension, duration of combat and specific non-combat stress of varying intensity, all of which often exceed human capabilities for psychological resilience. The loss of comrades and participation in violence against the enemy are traditional triggers for PTSD. In hybrid campaigns like in Ukraine, effects are enhanced against a background of complex ethnonational identities. At the same time, the extent of outside stressors and their geographical scope pull social fabrics apart along targeted cleavages, leaving individuals with no firm idea of where they belong and what to believe in terms of current events and future goals. Called into question are ideas of a peaceful environment, standard values of society, and assessments by peaceful citizens of participants in hostilities.

In Ukraine, citizens must contend with competing narratives that the conflict in Donbas and Luhansk is the result of Russian incursion, a civil war between Ukrainians, the result of an ethnic division between Russians and Ukrainians, freedom fighters seeking independence from a corrupt Ukrainian government, or part of a larger expansion of power via “Novorossiia.” The lack of a dominant narrative is intentional. The less agreement there is on the nature of the conflict, its causes, and how to assess those fighting it, the more stress and division can be caused within the non-combat areas of Ukraine and neighboring countries. In contrast to the strengthening of collective identities in the face of a clear aggressor (the American ideal of the Second World War), in a hybrid war, no one knows who the aggressor really is or why. Peace could come at any time or never, history becomes gaslit, and a sense of stability becomes ephemeral.⁴⁵

The population’s potential to protest against or support the conflict can also be used as an inroad for hybrid warfare exploitation in the target country. Frustrations and resentments borne from the larger conflict, coupled with perceptions of corruption or malfeasance among political, military, and business leaders, can easily be intensified by various cyber campaigns and targeting. The deterioration of the social and economic conditions and lack of opportunities to change lives for the better can be reflexively controlled to alter election outcomes or to spark migration from one region to another. Migrants can then be targeted as part of an ethnic or cultural “invasion” to alter political feelings in a third country. This phenomenon has been witnessed both within Ukraine in dealing with internally displaced people from Crimea/Donetsk/Luhansk, and then in stoking resentment against Ukrainians migrating to countries like Poland. Russian media disinformation campaigns have worked against Syrian refugees in

PTSD Diagnostic by Identifying Ophthalmological Biomarkers,” *International Journal of Research and Innovation in Applied Science* 4, no. 2 (January 2019): 7-11, www.rsicinternational.org/journals/ijrias/DigitalLibrary/Vol.4&Issue1/07-11.pdf.

⁴⁵ Joanna Szostek, “Nothing Is True? The Credibility of News and Conflicting Narratives during ‘Information War’ in Ukraine,” *The International Journal of Press/Politics* 23, no. 1 (January 2018): 116-35, <https://doi.org/10.1177/1940161217743258>.

Germany and Latin American migrants in the United States by false stories planted and shared widely among domestic sources in Germany and the US.⁴⁶

Cybersecurity Threats from the COVID-19 Pandemic in the Context of Hybrid Warfare and Cyber-Social Vulnerabilities

The COVID-19 pandemic is an acute test of the effectiveness of healthcare systems around the world and the capacity of state, local, and national governments to meet the relevant security challenges and threats. While the understandable focus of the coronavirus pandemic remains primarily on the direct health impact on populations and the response to economic effects, the outbreak has suddenly shifted societies' interactions based on information technologies. While cyber systems and information technologies may provide some positive opportunities, certain systemic security risks and vulnerabilities must also be identified and addressed from the perspective of hybrid warfare.

An immediate impact of the COVID-19 pandemic in China was not only to seal off cities from one another and a complete lockdown of the city of Wuhan, but the imposition of mandatory tracking apps on personal phones. South Korea sent texts detailing the movements of people suspected to be infected, raising serious privacy and accuracy concerns.⁴⁷ These tracking policies reflect technological capabilities and tracking movements in helping to predict the spread of infectious diseases like the coronavirus. Still, these were applied against the backdrop of concerns over homeland security, individual privacy, and potential exploitation by either government or nongovernment actors, especially with the regional and geopolitical transformations caused by the COVID-19 pandemic.

The European Commission announced its intention to track the movement of citizens through mobile technology in 2020. Thierry Breton, European Commissioner for Domestic Market and Services, assured that the EU plan did not have the goal of controlling people, and the data would remain anonymous and be deleted by the end of the pandemic. The European Data Protection Supervisor stated that this decision did not violate confidentiality rules. Vodafone, Deutsche Telekom, Orange, Telefonica, Telecom Italia, Telenor, Telia, and A1 Telekom Austria agreed to provide the data. In Germany, such surveillance was prohibited by law. Still, the COVID-19 pandemic opened a discussion about the need to intervene in the fundamental rights of citizens, especially by a state already imposing significant restrictions on freedom of movement. Jens Spahn, German Minister of Health, was the first to propose collecting data from the mobile phones of

⁴⁶ Stefan Meister, "The 'Lisa Case': Germany as a Target of Russian Disinformation," *NATO Review*, July 25, 2016, <https://www.nato.int/docu/review/2016/Also-in-2016/lisa-case-germany-target-russian-disinformation/EN/index.htm>; Howard et al., "The IRA, Social Media and Political Polarization."

⁴⁷ Oleg Matyevchev, "What Did China Get in the Last Three Months," *LiveJournal*, March 20, 2020, accessed April 5, 2020, <https://matveychev-oleg.livejournal.com/9896483.html>. – in Russian.

infected individuals.⁴⁸

Deutsche Telekom has already provided information on millions of its customers to the Robert Koch Institute (RKI). RKI specialized in the study of infectious diseases and was central in discussions about information policy concerning the COVID-19 pandemic. Virologists at RKI hoped to construct maps of the movements and German residents and understand how long people in urban environments were exposed during the pandemic lockdown. All such information made it possible to predict infectious disease spread more accurately; it also allowed building a system for quickly calculating all the social connections of a given individual: who the person was in contact with, who was traveling with the person, where he/she was, and with whom they spoke.⁴⁹ For example, such mass surveillance systems have been introduced in countries such as China and Russia. In Russia, Prime Minister Mikhail Mishustin proposed systems to track all individuals suspected of being infected with COVID-19 by geolocation of their mobile phones. Many countries have also proposed new surveillance programs to better plan for hospital needs and available resources. However, this required a significant relaxation of medical data confidentiality and demonstrated a blurring of the lines between privacy, the public good, and whether the institutions that hold such information can be trusted.⁵⁰

Trust, Fakes, and Disinformation

The issue of trust moves beyond that of individual governments. In disaster situations, verifiable information is always a valuable commodity, and in prolonged stress situations, people become more vulnerable to innuendo, rumor, and deliberate disinformation. The ease of such disinformation spreading across the globe is greatly amplified by modern information networks, from instant communication apps to social media. The COVID-19 pandemic has created fertile ground for developing and spreading conspiracy theories. Where information is lacking, and uncertainty is high, this vacuum is easily filled with disinformation and unverifiable stories.⁵¹ The coronavirus presents particular problems concerning disinformation: the long incubation period, the fact it can be spread by asymptomatic people, the international origins of the virus, combined with the

⁴⁸ Foo Yun Chee, "Vodafone, Deutsche Telekom, 6 Other Telcos to Help EU Track Virus," *Reuters*, Technology News, March 25, 2020, accessed April 1, 2020, <https://uk.reuters.com/article/us-health-coronavirus-telecoms-eu/vodafone-deutsche-telekom-6-other-telcos-to-help-eu-track-virus-idUKKBN21C36G>.

⁴⁹ "Geolocation Surveillance: What Is Allowed in Germany for the Fight Against Coronavirus," *DW Made for Minds Journal*, April 2020.

⁵⁰ Radu Mîrza, "COVID-19 and Digital Rights in Romania, Moldova and Ukraine," *Central and Eastern European EDem and EGov Days* 341 (March 2022): 195-211, <https://doi.org/10.24989/ocg.v341.14>.

⁵¹ Sally McManus, Joanna D'Ardenne, and Simon Wessely, "Covid Conspiracies: Misleading Evidence Can Be More Damaging Than no Evidence at All," *Psychological Medicine*, no. 1-2 (2020), <https://doi.org/10.1017/S0033291720002184>.

public health policy dilemma of proving a negative. Model projections of potential deaths can be altered by significant social distancing, and the original warning estimates can be overstated. Economic costs are more obvious and immediate, while public health benefits are largely ephemeral until lost.⁵²

One of the main conspiracies associated with the coronavirus was that it is of artificial and deliberate origin, created in the laboratory of some country. The 2019 dispute over China's researcher at the National Microbiology Lab in Winnipeg served as a basis for false claims that the Canadian government had created the virus, which was then stolen and released by a Chinese researcher.⁵³ Canadian disputes with the Chinese telecom company Huawei also became part of conspiracy theories, asserting that 5G networks are responsible for the spread of the virus. Picked up in Britain, the 5G conspiracy has resulted in attacks on numerous cell phone network towers.⁵⁴ In many countries during 2020-2022, a variety of information about the pandemic was disseminated, both with significant inaccuracies and mis/disinformation.⁵⁵ This often-controversial information has been featured in many official briefings and news networks, covering almost every aspect of COVID-19.⁵⁶

Conflicting messages in public policy responses, information, and media commentary in virtually every country have created considerable confusion about the extent of the risks associated with the pandemic, with sharp divisions over the danger from the virus. Some theories have centered on how some figures have used the media to conspire to undermine the authority of certain politicians or medical experts and that claims of potential infection and death from COVID-19 have been greatly exaggerated. Such patterns of disinformation in Ukraine have caused more than just stress and uncertainty. Thus, one should recall the violent protests in Ukraine that broke out in February 2020 based on false information about the risks of the spread of the virus by citizens returning from China. Social media disinformation about the pandemic circulated in Ukraine throughout 2020-2021 and significantly hampered government efforts.

The disinformation messages are therefore tailored to amplify uncertainty and sow doubt. Texts and messages are often presented in a trusting manner,

⁵² Edward Lucas, "Mutations of Misinformation," *Tyzhden.ua*, March 1, 2020, accessed 5 April 2020, <https://tyzhden.ua/Columns/50/240946>.

⁵³ Dax Gerts et al., "'Thought I'd Share First' and Other Conspiracy Theory Tweets from the COVID-19 Infodemic: Exploratory Study," *JMIR Public Health and Surveillance* 7, no. 4 (April 2021): e26527, <https://doi.org/10.2196/26527>.

⁵⁴ Takele T. Desta and Tewodros Mulugeta, "Living with COVID-19-Triggered Pseudoscience and Conspiracies," *International Journal of Public Health* 65, no. 6 (2020): 713-714, <https://doi.org/10.1007/s00038-020-01412-4>.

⁵⁵ Sahil Loomba et al., "Measuring the Impact of COVID-19 Vaccine Misinformation on Vaccination Intent in the UK and USA," *Nature Human Behaviour* 5, no. 3 (2021): 337-348, <https://doi.org/10.1038/s41562-021-01056-1>.

⁵⁶ Emily Chen et al., "COVID-19 Misinformation and the 2020 U.S. Presidential Election," *Harvard Kennedy School (HKS) Misinformation Review*, March 3, 2021, <https://doi.org/10.37016/mr-2020-57>.

with an address to a close personal acquaintance. They usually contain all the information about something that may excite the recipient but also include a call to action. Individuals are told what to do to protect themselves; they are also asked to spread this “secret” invaluable information to help as many other people as possible. Often the motive behind such reports is the assertion that authorities are hiding either solutions to the pandemic or its sources. The source of this information is generally not specified and is usually included in the narrative as an expert and acquaintance. The sources of information may either be foreign, intending to create disorder, or maybe domestic actors with a financial interest in spreading disinformation. PRC disinformation efforts visibly shifted in 2020 to target individual phone text users in the US, specifically to spread COVID-related disinformation.⁵⁷

Disinformation campaigns have long-term consequences not only directly to individuals who may take harmful actions but are also damaging the social and political fabric in environments where verifiable and false information cannot be distinguished. Information technology in the decentralization of news sources makes the rapid dissemination of false information nearly uncontrollable and very difficult to overcome. After the Chernobyl incident in 1986 in Ukraine, it was often said that hundreds were killed by radiation and many thousands by information. In a pandemic, it is difficult to quantify the number of casualties associated with inaccurate information, mis- or disinformation, but conservative estimates indicate that thousands of lives could have been saved with more timely government intervention and public health action.⁵⁸

Such intense cyber informative influences cause a stressful state for many people, which is maintained for a long time with varying intensity. This condition can be described as “pandemic information stress,” which in the future may be exposed to various psychosomatic changes: post-traumatic stress disorders (PTSD), the development of anxiety-depressive states, panic attacks, the formation of phobias, and obsessive-compulsive disorders consequences. Their emergence and evolution are significantly influenced by the state of the economy, the threat of lowering living standards, unemployment, and insecurity in the future.⁵⁹ The global trend has become a replication of false information on social networks, the distribution of photos and videos without a clear context

⁵⁷ Edward Wong, Matthew Rosenberg, and Julian E. Barnes, “Chinese Operatives Helped Sow Panic in U.S., Officials Say,” *The New York Times*, April 23, 2020, A10.

⁵⁸ Nicholas Charron, Victor Lapuente, and Andrés Rodríguez-Pose, “Uncooperative Society, Uncooperative Politics or Both? How Trust, Polarization and Populism Explain Excess Mortality for COVID-19 across European Regions,” The QoG Institute Working Paper 12 (Göteborg, Sweden: The Quality of Government Institute, Department of Political Science, University of Gothenburg, December 2020), <http://hdl.handle.net/2077/67189>.

⁵⁹ Ali Farooq, Samuli Laato, and AKM Najmul Islam, “Impact of Online Information on Self-Isolation Intention during the COVID-19 Pandemic: Cross-Sectional Study,” *Journal of Medical Internet Research* 22, no. 5 (2020): e19128, <https://doi.org/10.2196/19128>.

but with a clear emotional focus, the reliability of which is difficult to assess at the time of viewing. During a pandemic, such informational effects have particularly severe social consequences and become a powerful tool of hybrid warfare.

Cyber Crimes and Espionage

A related yet distinct issue is the intensification of cybercrime. Some crimes are directly related to medical institutions and their information systems. For example, criminals are looking for information about drugs, tests, or vaccines related to coronavirus for sale on the black market. Another trend is the circulation of counterfeit so-called coronavirus drugs and the open market, considering everyone's familiarity with the virus and intense desire to avoid infection. In addition, destructive cyber actions aim at violating medical institutions' health facilities and stealing confidential data. Some attempts also include the encryption of large volumes of critical medical data to obtain ransom for their restoration. The pandemic has opened hospitals, research centers, and universities to attacks by organized cyber criminals. Attacks were carried out against the University Hospital in Brno, Czech Republic, a major COVID-19 testing center, the British Hammersmith Medicines Research, which develops COVID-19 vaccines, AP-HP Paris Hospital, and a number of Spanish hospitals. In addition, the World Health Organization (WHO) warned of suspicious e-mails received from attackers trying to take advantage of the emergency to steal money and confidential information, as well as attempts to hack into WHO's computer systems and its coronavirus database.⁶⁰ European Commission President Ursula von der Leyen has warned that cybercrime in the EU has increased due to the coronavirus outbreak. "They follow us on the Internet and use our fears about the coronavirus. Our fear is becoming their business opportunity," EU Observer reported.⁶¹

The sudden shift to remote working and banking also exposes many people to theft through financial systems or commercial and industrial networks that were never intended to be widely distributed. One fear among cyber security experts has been that businesses will take shortcuts in their network security in order to maintain profits during the severe economic downturn. Commercial and industrial information will be shared across private networks and on personal computers, with IT security unable to police the use of these open networks. For countries already at risk for acts of industrial espionage before the pandemic, cybercriminals and outside actors will not fail to see the opportunities available to them.⁶²

⁶⁰ World Health Organization, "Beware of Criminals Pretending to be WHO," April 2020, accessed April 5, 2020, <https://www.who.int/about/cyber-security>.

⁶¹ "The EU Recorded a Sharp Increase of Cybercrime: What Is Happening," *Informacione Sopotivlenie*, March 25, 2020, accessed April 1, 2020, <https://sprotiv.info/analitica/v-es-zafiksirovali-rezkij-rost-kiberprestupnosti-chto-proishodit>.

⁶² Eduard Babulak, James C. Hyatt, Kim Kyu Seok, and Jang Sun Ju, "COVID-19 & Cyber Security Challenges US, Canada & Korea," *Transactions on Machine Learning and Data*

Education and Transition to E-Learning

Education is another critical issue directly related to the pandemic and cyber-social vulnerabilities in hybrid warfare conditions. Due to COVID-related quarantines, there were crucial changes in the established rhythms of life, work, and study of all segments of the population in almost all countries. For the first time, humanity faced a pandemic of this level in the context of a high-tech information society, globalization, and easily accessible global travel. Business, tourism, migration activity, and population mobility were disrupted overnight. The forced, real, rapid, and massive transition to e-learning in all spheres and at all levels of education became stressful for all participants of the educational process, who were forced to master new tools and methods hastily.

Education under pandemic conditions has become a strategic issue with far-reaching implications for the whole world. UN Secretary-General António Guterres noted that about one billion students and schoolchildren in 160 countries worldwide could not receive full education due to the closure of educational institutions caused by the coronavirus epidemic. It threatens the world with a “generational catastrophe.” According to polls conducted in Ukraine in July 2020 and estimates by the State Service for the Quality of Education of Ukraine, e-learning in schools is not supported by 48% of parents and 45% of students, whereas only 9.9% of the respondents “fully support” e-learning.⁶³

The problems lie not only in the essence of e-learning but also in the socio-technical contradictions and cyber-social vulnerabilities associated with it. E-learning is multifaceted and multidisciplinary. The issue includes technical, social, demographic, psychological, content-informational, methodological, didactic, organizational, cyber, and other aspects, as well as the ability of governments to train personnel for developing and delivering e-learning. The students must be prepared for the correct and effective use of technologies while protecting their mental and physical health in uncertain and stressful conditions.

Educational issues that have arisen in the context of hybrid confrontation and pandemic directly affect all spheres of state functioning and areas of national security. In general, this is a question of the fate of the state and the statehood of their further existence and development. In the absence of government control and regulation, e-learning can potentially lead not only to an increase in inequality in education and the loss of human potential but also to perilous changes in information processing, critical thinking, and social media dependence that may leave them vulnerable to cognitive and emotional cyber warfare techniques.

Mining 13, no. 1 (2020): 43-59, http://www.ibai-publishing.org/journal/issue_mldm/2020_October/13_2_43_59_mldm.pdf.

⁶³ Yuriy Danyk and Tamara Maliarchuk, “Strategic Aspects and Problems of E-learning in the Context of Pandemic and National Security,” *S-Direct* 24 3, no. 14 (July 2020), International scientific journal published under the auspices of NATO Defence Education Enhancement Program.

The pandemic has generated a demand for official e-learning standards for training specialists and the development of e-learning courses, which will help evaluate the e-learning processes' effectiveness and promote the systemic approach in a new mode of education in countries from the United States to Ukraine. It means that e-learning requires standardization, systematization, and strategic approaches to ensuring effective remote education while providing resources to deliver aims on a tactical institutional level. Even though the pandemic will end sooner or later, education (civil, government, and military) is unlikely to return to its former normalcy, and the implications for national security must be considered. COVID-19 has forced enormous and sudden changes upon societies, and our dependence upon technology requires intelligent public policy decisions concerning not only response to the virus itself but recognizing the vulnerabilities that technologies introduce.

Conclusion

This article aimed to outline the main problems caused by hybrid warfare, COVID-19, and possible solutions in cyberspace, social life, and national security that impact all spheres of state functioning. Exploiting cyber-social vulnerabilities plays a special and increasing role in hybrid conflicts. The creation of effective national cybersecurity and cyber defense system of the state, including the characteristics of cyber-social vulnerabilities, is one of the most important priorities in ensuring national security and defense. Effective early warning of cyber-social vulnerabilities requires structural and parametric analysis of cyber systems and their users and an understanding of how messages propagate, are received, and reproduced in cyber ecosystems. Strategies for increasing the resilience of information systems rely not only on "citadel" models of keeping intruders out but how to prepare populations for tricks, hacks, and disinformation campaigns from within and external agents.

The primary strategic aims of hybrid warfare tend to be destabilizing – that is, not the physical occupation of territory but sowing distrust in institutions and information itself. Such attacks have a destructive impact not only on critical infrastructure but also on society. It was established that the main destructive cyber actions were carried out selectively and focused on vulnerable cyber-social elements. The use of destructive focused cyberattacks was carried out as a part of large-scale complex cyber operations.

The main problems arising or manifested in connection with the COVID-19 pandemic in the context of hybrid warfare are as follows:

- Insufficient readiness of cyber-social health care systems of most countries;
- Significant restructuring of major national economic processes as a result of COVID-19 responses and the formation of new models of life and society;

- Rapid and complete immersion of the population in cyberspace and the transition to remote, distant modes of work and study;
- Growth of activity in social networks, increase in volumes of online trade, streaming entertainment, and online services (e.g., telemedicine, e-learning, e-banking);
- An increase in a wide range of cybercrimes, the spread of fake news related to the pandemics, misinformation, and information oversaturation of society;
- Insufficient level of cyber information literacy, inability or unwillingness to use Internet systems and IT technologies in everyday life, and failure to ensure cyber and information security, especially in the context of the global hybrid war.

While we have previously discussed developments in cyber-hybrid warfare, the COVID-19 pandemic has accelerated both activities and vulnerabilities associated with privacy, isolation, shifting identities, and propagation of disinformation.⁶⁴ The pandemic has allowed the further intrusion of destabilizing actors into people's lives, higher dependence on virtual information as traditional social ties have been disrupted, and further reliance on cyber technologies for all aspects of life.

The introduction of control over the implementation of quarantine requirements with the use of high-tech means deserves special attention. Failure to take precautionary measures to protect the rights of citizens in a timely manner is likely to violate the confidentiality of personal information. There is reason to predict that such control and supervision of citizens and their activities in many countries, especially with authoritarian regimes, may not only remain but even intensify once the pandemic subsides. Such a progression poses a threat to one's home country and provides inroads for outside actors to exploit and leverage such "social credit" systems to their benefit. The more dependent we become on such technologies, the more vulnerabilities allow the exploitation of such linkages, now largely independent of traditional social resilience. What are the security implications of cases when outsiders change medical records, place people on "no-fly" lists, or spoof their identity not only for loan applications but in worldwide media?

The COVID-19 pandemic has shocked the global system, not only in terms of economic activity and cross-border travel, but in how we relate to technology, how we measure and value social and political resilience, and our abilities to respond to the spectrum of hybrid warfare attacks that exploit cyber technologies and vulnerabilities. Our societies become ever more vulnerable to cognitive and emotive warfare that overwhelms our information processing, bypasses rational

⁶⁴ Tamara Maliarchuk, Yuriy Danyk, and Chad Briggs, "Hybrid Warfare and Cyber Effects in Energy Infrastructure," *Connections: The Quarterly Journal* 18, no. 1-2 (2019): 93-110, <https://doi.org/10.11610/Connections.18.1-2.06>.

thought, and hits us at a basic “survival” level, often as part of a strategy to further divide our societies and put institutions into question. While we have long expected cyber-hybrid warfare to become more important, it is now critical to address deficiencies in disinformation, privacy, cybercrime, and e-learning, all of which can affect larger questions of security and stability.

Thus, the research promoted the definition of Cyber War or Cyber Conflict in cyberspace and (or) through cyberspace. The confrontation in cyberspace and (or) through cyberspace is a complex socio-political phenomenon employing cyber intelligence, cyber defense, and cyber weapons for causing various losses to the enemy in different fields and minimizing own losses in economic, military, political, social, cyber, information, ideological, and other spheres. Unlike other destructive influences, conflicts, and (or) wars, cyber warfare (cyber conflict, destructive cyber actions) is not proclaimed. And if it begins, it does not end, being conducted continuously until one of the parties of the conflict is completely defeated or unable to continue the destructive actions. It can be completed only in case of the destruction of cyberspace.

While military strategies remain in place, the soft underbelly of society is increasingly under assault.

Disclaimer

The views expressed are solely those of the 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.

About the Authors

Dr. **Chad Briggs** is an Associate Professor and Director of Public Policy and Administration at the University of Alaska Anchorage. Dr. Briggs has field experience in information and hybrid warfare and in developing defensive strategies to protect critical systems in Eastern Europe and the Balkans. He has a Ph.D. in political science from Carleton University in Canada. He has been previously a senior advisor for the US Department of Energy and the Minerva Chair and Professor of Energy and Environmental Security for the US Air University (USAF). He is the author (with Miriam Matejova) of *Disaster Security: Using Intelligence and Military Planning for Energy and Environmental Risks*.

E-mail: chad.briggs@alaska.edu

Major General **Yuriy Danyk**, Professor, Doctor of Engineering Sciences, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute.” Dr. Danyk is an expert in the art of war, national defense and security, information and cybersecurity, electronic and IT technologies, the design and application of robotic complexes, and special forces development. He has combat experience in the application of advanced defense technologies in the conditions of modern war.

E-mail: zhvinau@ukr.net

Dr. **Tamara Maliarchuk** was a member of the NATO working group on DEEP program implementation in the Armed Forces of Ukraine. She was an analyst with the S. Korolov Zhytomyr Military Institute in Ukraine and has worked with US forces on language and cyber defense. She conducts research in e-learning, innovative technologies in PTSD detection and therapy, and manipulative technologies in the web environment.

E-mail: maliarchuktamara@gmail.com



Maritime Cyber(in)security: A Growing Threat Imperils EU Countries

Yavor Todorov

Ph.D. program, Bulgarian Naval Academy, <http://www.naval-acad.bg/>

Abstract: The massive incorporation of advanced information and communication technologies in ships, ports, traffic, and cargo management increases efficiencies but also creates vulnerabilities. Various malicious actors are willing to exploit access through the cyber domain to gain certain benefits. This article examines cyber risks and threats in the maritime cyber domain and reviews applicable European, US, and international norms, standards, and frameworks aiming to promote cybersecurity. The author outlines six lines of effort focusing on information sharing, awareness raising, certification, and resilience.

Keywords: maritime security, cybersecurity challenges, norms, harmonization, frameworks, information sharing, awareness, training, resilience.

The world is changed. I feel it in the water. I feel it in the earth. I smell it in the air. Much that once was is lost.¹

Background

The maritime domain has grown significantly in the past ten years. It is currently a vast interconnected network of cargo ships, crude oil tanks, chemical tankers, container ships, passenger ships, insurance companies, offshore and shore operators, national and international authorities, military forces, navigation experts, maritime management, satellite, and communication systems. Today, the

¹ J.R.R. Tolkien, *The Lord of the Rings: The Fellowship of the Ring* (London, UK: HarperCollins Publishers, 2003).

maritime domain directly affects economic, political, and demographic dynamics on a global scale.

Catastrophic events are not foreign to the maritime industry. The Titanic, for example, sank in 1912, killing 1 517 people. However, as the maritime domain increasingly incorporates information and communication technologies (ICTs), the chance of catastrophe increases exponentially. These ICTs support essential shipping services such as navigation, engine monitoring, access control, entertainment, communication, and crew management. However, digitalization increases risks such as port or ship shutdowns, manipulation of essential services, and mass destruction, disorder, or loss of human life. These risks affect everyone, including private companies, governments, and individuals. As noted by Kathy Metcalf, president and chief executive officer of the Chamber of Shipping of the United States of America, the maritime industry remains vulnerable to cyberattacks, which could provoke catastrophic events, such as the takeover of a ship and ramming it into the Verrazano-Narrows Bridge.² This danger is confirmed by the increase of cyberattacks targeting the maritime domain by 400 percent in 2020.³

The maritime cybersecurity domain is regulated by many international and national public and private entities, such as the International Maritime Organization (IMO), the European Union Agency for Cybersecurity (ENISA), and the Baltic and International Maritime Council (BIMCO). Unfortunately, these organizations do not possess sufficient technical and human capabilities to implement, certify, and monitor the shipping cybersecurity system. Nor do they have adequate policies and procedures to enforce specific requirements.

The current regulatory framework cannot minimize the risks and threats primarily because there is no harmonization between the existing cybersecurity standards and procedures that monitor the maritime sector. IMO's International Safety Management Code, IMO's Guidelines on Maritime Cyber Risk Management, the EU's relevant guidelines, and the corresponding national norms are too broad, and the operators cannot achieve a resilient shipping cybersecurity system.

Another challenge is the lack of standardization of cybersecurity protocols across ships of different nations. This is due to the number of vessels operating in different environments and under various national flags. These vessels tend to follow minimal existing standards and ignore national maritime authorities' requirements.⁴

² John Grady, "Experts: Maritime Industry Remains Vulnerable to Cyber Attacks," *USNI News*, September 28, 2020, <https://news.usni.org/2020/09/28/experts-maritime-industry-remains-vulnerable-to-cyber-attacks>.

³ "Greater Cyber Security Needed for Coronavirus and Economic Crises," *Hellenic Shipping News*, May 6, 2020, <https://www.hellenicshippingnews.com/greater-cyber-security-needed-for-coronavirus-and-economic-crises/>.

⁴ Jeff Spivey, "Security by Design," *United States Cybersecurity Magazine* (Fall 2017), <https://www.uscybersecurity.net/csmag/security-by-design/>.

Many ships' informational infrastructure is set up following the "cybersecurity by design" approach. Based on this model, cybersecurity is included in the ship from its initial design and is addressed at every stage of the building process. However, this "by design" approach focuses on early warning and prevention instead of remediation and restoration after a security incident.⁵ As the current attack vectors are multidimensional and use state-of-the-art tools to infiltrate systems, this model creates significant risks and challenges for the shipping industry.⁶

Numerous different equipment and service providers allow each vendor to implement unique security protections, making harmonization a significant challenge. Additionally, publicly accessible systems required to identify and locate a vessel in distress also use this technology.⁷

The potential for cyberattacks to disrupt the shipping industry is high and could provoke catastrophic damage to vessels and critical infrastructure. It is crucial that ship owners, crews, and responsible organizations enhance cybersecurity awareness in the maritime industry. Following are well-grounded recommendations for enhancing international maritime cyber security regulations, policies, and frameworks to address the current cybersecurity challenges.

The Current State of the Maritime Domain

Global seaports are increasingly important to the world economy and the European Union (EU) economy. They are the main intersections of the world trade network, as they account for about three-quarters of EU freight trade with third countries and over one-third of intra-EU freight transport.⁸

Since 1970, the world maritime trade has increased steadily, both in volume and ship size. The United Nations Conference on Trade and Development (UNCTAD) expects maritime trade volumes to expand to an annual rate of 2.4 percent by 2030. Around two-thirds of global trade in goods occurs in developing countries, accounting for sixty percent of global goods transport. Much of this growth has been in East Asia, especially China. There has also been a surge in volumes on the Transpacific trade route linking East Asia to North America.⁹

⁵ Reciprocity, "What is Security by Design?" *Reciprocity*, March 7, 2020, <https://reciprocity.com/resources/what-is-security-by-design/>.

⁶ Rory Hopcraft and Keith M. Martin, "Effective Maritime Cybersecurity Regulation – the Case for a Cyber Code," *Journal of the Indian Ocean Region* 14, no. 3 (2018): 354-366, <http://doi.org/10.1080/19480881.2018.1519056>.

⁷ Hopcraft and Martin, "Effective Maritime Cybersecurity Regulation."

⁸ Boyan Mednikarov, Yuliyana Tsoneva, and Andon Lazarov, "Analysis of Cybersecurity Issues in the Maritime Industry," *Information & Security: An International Journal* 47, no. 1 (2020): 27-43, <https://doi.org/10.11610/isij.4702>.

⁹ United Nations Conference on Trade and Development (UNCTAD), *Review of Maritime Transport 2021* (United Nations, 2021), <https://unctad.org/webflyer/review-maritime-transport-2021>.

Maritime Cybersecurity Domain Analysis

Maritime industry progress relies heavily on technological innovation in digitalization aboard ships. Information systems grow more critical by the day as they facilitate communication and decision-making, enhance visibility, efficiency, and reliability, and increase security in shipping operations under various conditions.

Year	Tanker Trader	Main bulk	Other dry cargo	Total (all cargoes)
1970	1 440	448	717	2 605
1980	1 871	608	1 225	3 704
1990	1 755	988	1 265	4 008
2000	2 163	1 186	2 635	5 984
2005	2 422	1 579	3 108	7 109
2006	2 698	1 676	3 328	7 702
2007	2 747	1 811	3 478	8 036
2008	2 742	1 911	3 578	8 231
2009	2 641	1 998	3 218	7 857
2010	2 752	2 232	3 423	8 408
2011	2 785	2 364	3 626	8 775
2012	2 840	2 564	3 791	9 195
2013	2 828	2 734	3 951	9 513
2014	2 825	2 964	4 054	9 842
2015	2 932	2 930	4 161	10 023
2016	3 058	3 009	4 228	10 295
2017	3 146	3 151	4 419	10 716
2018	3 201	3 215	4 603	11 019
2019	3 163	3 218	4 690	11 071
2020	2 918	3 181	4 549	10 648

Figure 1: International Maritime Trade 1970-2020.¹⁰

A major event in 2017 changed how governments and private industry approach shipping and port cybersecurity systems. In June, hackers working for the Russian military security service distributed the *NotPetya* ransomware to critical infrastructure entities. By exploiting vulnerabilities in Maersk, the world's largest shipping conglomerate, the hackers impaired the Global Maritime Transport System.¹¹

¹⁰ UNCTAD, *Review of Maritime Transport*.

¹¹ Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, August 22, 2018, www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Following this attack, IMO published the Guidelines on Maritime Cyber Risk Management.¹² These guidelines recommend best practices regarding essential shipping services such as bridge systems, cargo handling, management systems, propulsion and machinery management, power control systems, access control systems, passenger servicing, and communication systems.¹³ These services run on the following platforms:

- ECDIS (Electronic Chart Display and Information System)
- AIS (Automatic Identification System)
- Radar/ARPA (Radio Direction and Ranging/ Automatic Radar Plotting Aid)
- Compass (Gyro)
- Steering (Computerized Automatic Steering System)
- VDR (Voyage Data Recorder)
- GMDSS (Global Maritime Distress and Safety System)
- ESD (Emergency Shut Down Systems).

Technical analysis showed the following vulnerabilities in some of these systems.¹⁴

Table 2. Shipping Platforms Threat Analyses.¹⁵

Platform	Use	Vulnerability	Impact
ECDIS	Visualization of navigation charts	Lack of mechanism for authentication	Altering the route
AIS, GMDSS	Identification and distress alert	Not equipped with security and data verification mechanisms	Generating false AIS command commands and altering the ship’s route
Emergency Shut Down Systems (ESD)	Block the propulsion and machinery management in case of emergency	Accessible from the shore	The vessel’s machine could be stopped remotely

Source: Mednikarov et al., 2020.

¹² International Maritime Organization (IMO), “Maritime Cyber Risk,” www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx.

¹³ IMO, “Maritime Cyber Risk.”

¹⁴ Mednikarov, Tsonev, and Lazarov, “Analysis of Cybersecurity Issues in the Maritime Industry.”

¹⁵ Mednikarov, Tsonev, and Lazarov, “Analysis of Cybersecurity Issues in the Maritime Industry.”

In addition, many of the new software products are not compatible with the hardware used. The most common operating system on merchant ships is Windows XP, although support from Microsoft expired in 2014. In 2015, a study in the United States found that thirty-seven percent of servers were not up-to-date and were considered potentially vulnerable to cyberattacks.¹⁶ In 2020, these numbers were similar, as the main ship's equipment had not changed.

The main types of cyberattacks against vessels exploiting existing vulnerabilities are:

- Phishing – Sending e-mails to a large number of addressees, requiring them to fill in sensitive or confidential information. Such attacks may also prompt the user to access a particular resource to allow unauthorized access to the information infrastructure.
- Ransomware – Actions where malicious code encrypts stored data in a system and requires a ransom to decrypt it. Vessels are vulnerable to this because they lack plans for checking the files used, and most of them lack mechanisms for checking incoming and outgoing electronic correspondence.¹⁷
- Scanning – The process of finding vulnerabilities in a particular system.
- Denial of service – The process by which the traffic of a certain number of remotely controlled computers overloads the communication capacity or interrupts access to a particular resource or service.
- Supply chain attack – The process of malicious influence on a ship's systems through a device in which malicious code is pre-injected.
- GPS Spoofing – The process when an attacker tricks the ship's GPS receiver into changing the location display to another.
- Man-in-the-middle attack – The process when the attackers can intercept and affect the traffic between the ship and shore.

The Baltic and International Maritime Council (BIMCO)'s Guidelines on Cybersecurity Onboard Ships¹⁸ outlines several cyber threat "actors" for ships. One type of actor is the activist. Their goal can be, among others, the destruction or publication of sensitive data to gain attention from the media or DoS (Denial of Service) and Intellectual property theft.¹⁹ This could include an insider threat that disrupts operational services and causes reputational loss. The second type

¹⁶ Ms. Smith, "Maritime Cybersecurity Firm: 37% of Microsoft Servers on Ships Vulnerable to Hacking," *CSO*, May 4, 2015, <https://www.csoonline.com/article/2917856/maritime-cybersecurity-firm-37-of-microsoft-servers-not-patched-vulnerable-to-hacking.html>.

¹⁷ Mohamed Amine Ben Farah et al., "Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends," *Information* 13, no. 1 (2022), 22, <https://doi.org/10.3390/info13010022>.

¹⁸ Baltic and International Maritime Council, 2020.

¹⁹ IMO, "Maritime Cyber Risk."

of actors are criminals seeking financial gain through both commercial and industrial espionage. The end goal is selling and ransoming stolen data, blocking system operability, and organizing fraudulent cargo transportation. The third group, and probably the most feared, are nation-state-supported groups seeking political or military influence by negatively interfering with the targeted vessel or shipping company’s essential services. A successful cyber-attack could be used to decrease the government’s authority or modify the state’s political goals and focus.²⁰ Nation-state actors tend to focus on the exfiltration of sensitive and classified data or influencing an essential service. They have almost unlimited resources and can achieve their goals without being limited by time horizons or potential financial profits. Examples of essential nation-state attacks include the cyberattacks on the election system in Estonia in 2007,²¹ the cyberattacks during the Russo-Georgian War,²² and the DDoS attacks on US banks in 2013.²³

The most significant examples of these types of cyberattacks are shown in the table below.

Table 2. Major Maritime Cyberattacks Examples.

Type of Attack	Year	Description
Ransomware attack/ phishing attack	2021	South Korea’s national flagship carrier HMM: Cyberattack, resulted in limited email system access. ²⁴
Ransomware attack	2020	Port near the strait of Hormuz: The attempted cyberattack damaged some operating systems at the port. ²⁵
Malware attack	2020	Mediterranean Shipping Company (MSC): For security issues, MSC servers were closed

²⁰ IMO, “Maritime Cyber Risk.”

²¹ Patrick Howell O’Neill, “The Cyberattack That Changed the World,” *Daily Dot*, May 20, 2016, <https://www.dailydot.com/debug/web-war-cyberattack-russia-estonia/>.

²² “The Russo-Georgian War 2008: The Role of the Cyber Attacks in the Conflict,” *AFCEA*, May 24, 2012, <https://www.afcea.org/committees/cyber/documents/therusso-georgianwar2008.pdf>.

²³ Nicole Perlroth and Quentin Hardy, “Banking Hacking was the Work of Iranians, Officials Say,” *The New York Times*, January 8, 2013, <https://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html>.

²⁴ Naida Hakirevic Prevljak, “HMM Hit by Cyber Attack,” *Offshore Energy*, June 15, 2021, <https://www.offshore-energy.biz/hmm-hit-by-cyber-attack/>.

²⁵ Tzvi Joffe, “Cyber Attack Targets Iranian Port near Strait of Hormuz,” *The Jerusalem Post*, May 11, 2020, <https://www.jpost.com/breaking-news/cyber-attack-targets-iranian-port-near-strait-of-hormuz-627616>.

		to protect the company's data, and, as a result, the company's website was taken down. ²⁶
Malware attack	2019	The attack targeted a US vessel, causing critical credential mining. The Coast Guard and the FBI reported that the lack of security on the ship was the main reason for such an attack: all crew on the vessel shared the same login and password for the vessel's computer. Moreover, the use of external devices facilitated the task of the hacker. Another critical mistake is the lack of antivirus software. ²⁷
Phishing attack	2019	Hackers obtained unauthorized access to James Fisher and Sons Plc (UK). ²⁸
Ransomware attack	2018	Chinese hackers had attacked US Navy contractors. ²⁹
Petya Ransomware	2017	The encrypted malware targeted all services of the Maersk shipping company. The attack named <i>NotPetya</i> affected computer servers in Europe and India. The attack severely destroyed the computers' operating system by infecting its master boot record (MBR). As a result, 17 shipping container terminals were affected, and more than 200 million USD were lost. ³⁰
GPS spoofing attack	2017	The attack is reported by US maritime administration. The GPS of a ship in the Russian port of Novorossiysk indicated a wrong localization. ³¹

²⁶ Marcus Hand, "MSC Confirms Malware Attack Caused Website Outage," *Seatrade Maritime News*, April 17, 2020, <https://www.seatrade-maritime.com/containers/msc-confirms-malware-attack-caused-website-outage>.

²⁷ Davey Winder, "U.S. Coast Guard Issues Alert after Ship Heading into Port of New York Hit by Cyberattack," *Forbes*, July 9, 2019, <https://www.forbes.com/sites/davey-winder/2019/07/09/u-s-coast-guard-issues-alert-after-ship-heading-into-port-of-new-york-hit-by-cyberattack/>.

²⁸ "Marine Firm James Fisher Reports Cyber Breach," *Reuters*, November 5, 2019, <https://www.reuters.com/article/us-james-fisher-cybercrime-idUSKBN1XF1SQ>.

²⁹ "China Hackers Steal Data from US Navy Contractor," *BBC*, 9 June 2018, <https://www.bbc.com/news/world-us-canada-44421785>.

³⁰ Greenberg, "The Untold Story of NotPetya."

³¹ David Hambling, "Ships Fooled in GPS Spoofing Attack Suggest Russian Cyberweapon," *NewScientist*, August 10, 2017, <https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/>.

Navigation systems attack	2017	A collision between the USS Fitzgerald and a container ship caused the death of seven sailors. (of the coast of Japan) ³²
GPS spoofing	2013	A research team at the University of Texas succeeded in spoofing a yacht's GPS receiver. ³³

Maritime Cybersecurity Legal Framework

To assess the factors that led to the current state of the maritime security system, we must first analyze the maritime cybersecurity framework. This section will demonstrate the unique challenges of maritime cybersecurity related to the lack of a coherent and efficient regulatory framework to minimize the risks and threats and enhance cyber resilience. It presents an overview of the international framework and the EU and US norms and regulations.

Overview of the International Maritime Cybersecurity Framework

Maritime security measures have usually been reactive to major global shocks or disasters, such as the adoption of the International Ship and Port Facility Security (ISPS) Code.³⁴ In response to threats to ships and ports, the ISPS Code entered into force in 2004 under Chapter XI-2 of the International Convention for the Safety of Life at Sea (SOLAS Convention), acknowledging the importance of ports in the global security domain and outlining a set of mandatory tools and recommendations to ships and port facilities.³⁵ This Code assumes that ensuring the safety of ships and ports is a risk management activity. Although this Code has some links to cybersecurity, such as the measures concerning access control and authentication requirements, it is primarily designed to address the physical security of the port facilities.

Another critical international norm, which has also been developed within IMO, is the Convention on Facilitation of International Maritime Traffic (FAL).³⁶ This convention, in force since 1967, is focused on increasing the efficiency of maritime transport. It standardizes forms to be used in the interchange of infor-

³² Sam LaGrone, "7 Sailors Missing, CO Injured after Destroyer USS Fitzgerald Collided with Philippine Merchant Ship," *USNI News*, June 16, 2017, <https://news.usni.org/2017/06/16/destroyer-uss-fitzgerald-collides-japanese-merchant-ship>.

³³ Brian Dodson, "University of Texas Team Takes Control of a Yacht by Spoofing Its GPS," *New Atlas*, August 11, 2013, <https://newatlas.com/gps-spoofing-yacht-control/28644>.

³⁴ International Maritime Organization (IMO), "SOLAS XI-2 and the ISPS Code," <https://www.imo.org/en/OurWork/Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx>.

³⁵ IMO, "SOLAS XI-2 and the ISPS Code."

³⁶ International Maritime Organization (IMO), "FAL Convention," 1967, www.imo.org/en/OurWork/Facilitation/Pages/FALConvention-Default.aspx.

mation in the maritime-port sector, particularly concerning communication between ports and ships.³⁷ In order to provide FAL with adequate applicability, it was updated in 2019. It included requirements that public authorities introduce systems that enable the electronic exchange of information between ships and ports.³⁸ A significant innovation of this convention is that it encourages the use of a “single window” concept, in which all the stakeholders exchange data via a single point of contact. The drawback is that if an attacker gains access to any of the entry points, he gains access to the whole network.

In 2017, IMO adopted resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management Systems (SMS).³⁹ The resolution states that an approved SMS should consider cyber risk management following the objectives and functional requirements of the International Safety Management Code (ISM Code).⁴⁰ It further encourages national authorities to ensure that cyber risks are appropriately addressed in Safety Management Systems in the company’s Document of Compliance as of January 1, 2021. If it is not addressed, the vessel is treated as not sea safe, and therefore, it is considered a global maritime threat.

A paramount IMO document explicitly addressing maritime cybersecurity is the IMO document entitled Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/ Circ.3), approved at the 41st session of the FAL Committee.⁴¹ Essentially, this document recognizes that the maritime domain needs to raise cybersecurity awareness and implement specific recommendations to enhance its cyber resilience.⁴² The guidelines do acknowledge that each stakeholder in the maritime industry is different. Therefore, each should implement the most relevant requirements stipulated by the flag state administration for their needs. The Guidelines⁴³ also encourage implementing international security standards such as ISO/IEC 27001,⁴⁴ which specify requirements for an information security management system. The Guidelines take note of industry best practices and incorporate five elements: identification, protection, detection, response, and recovery. A new element in this regulation is connected to the possibility of the vessel

³⁷ IMO, “FAL Convention,” 1967.

³⁸ International Maritime Organization (IMO), “FAL Convention,” 2017, www.imo.org/en/OurWork/Facilitation/Pages/FALConvention-Default.aspx.

³⁹ IMO, “Maritime Cyber Risk Management in Safety Management Systems,” Resolution MSC.428(98), adopted on June 16, 2017, [https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MS.428\(98\).pdf](https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MS.428(98).pdf).

⁴⁰ IMO, *ISM Code: International Safety Management Code with Guidelines for Its Implementation* (London, UK: IMO Publishing, 2018).

⁴¹ IMO, “Maritime Cyber Risk.”

⁴² Akash Rana, “Commercial Maritime and Cyber Risk Management,” *Safety & Defense* 5, no. 1 (2019):46-48, <https://doi.org/10.37105/sd.42>.

⁴³ IMO, “Maritime Cyber Risk.”

⁴⁴ International Organization for Standardization (ISO), “ISO/IEC 27001: Information Security Management,” 2013, www.iso.org/isoiec-27001-information-security.html.

being found unseaworthy if the recommendations are not implemented.⁴⁵ Although the IMO Guidelines on Maritime Cyber Risk Management offer recommendations to protect ships from current cyber risks and threats, they do not offer specific guidance on how to secure the communication channels between the port and vessel. Another major challenge is that the control over the implementation is linked to the flag state and the national maritime authority.⁴⁶

To enhance interoperability, IMO implemented, in collaboration with the International Electro-Technical Commission (IEC), a new standard for maritime navigation and radio-communication equipment and systems: IEC 63.154 “Cybersecurity – General Requirements, Methods of Testing and Required Test Results.”⁴⁷ This standard implements requirements, methods of testing, and standards for shipborne equipment to provide a basic level of protection against cyber incidents.

Overview of the European Union Maritime Cybersecurity Regulatory Framework

On the strategic level, the EU’s driving efforts are built around the EU Security Union Strategy for 2020-2025.⁴⁸ This strategy asserts that cyberattacks and cybercrime continue to rise, and its primary goals are to increase the whole-of-society approach to security. This includes sector-specific initiatives to tackle the specific risks faced by critical infrastructures such as transport and maritime.

The general effort to secure the EU’s maritime transport is supported by Directive (EU) 2016/1148, also known as the NIS Directive.⁴⁹ It was created to increase the security of networks, services, and information systems.⁵⁰ The NIS Directive aims to build cybersecurity capabilities across the EU, mitigate threats to network and information systems used to provide essential services in critical sectors and ensure the continuity of such services after cybersecurity incidents.⁵¹

⁴⁵ IMO, “Maritime Cyber Risk.”

⁴⁶ Nineta Polemi, *Port Cybersecurity: Securing Critical Information Infrastructures and Supply Chains* (Amsterdam: Elsevier, 2017).

⁴⁷ International Electrotechnical Commission (IEC), “IEC 63154:2021 – Maritime navigation and radiocommunication equipment and systems – Cybersecurity – General requirements, methods of testing and required test results,” accessed May 13, 2021, <https://webstore.iec.ch/publication/61003>.

⁴⁸ European Commission, “About the European Security Union,” https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_en.

⁴⁹ “NIS Directive – Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union,” Document 32016L1148, *EUR-Lex*, July 19, 2016, <https://eur-lex.europa.eu/eli/dir/2016/1148/oj>.

⁵⁰ “NIS Directive – Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016.”

⁵¹ “NIS Directive – Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016.”

It is stressed in the Directive that the growing interdependencies between the different essential services could disrupt entities and sectors and have cascading negative impacts on the delivery of services across markets. Accordingly, the member states' essential service operators should do everything in their power to manage the risks of being attacked and further report to the authorities if there is a cybersecurity breach.⁵²

The NIS Directive requires every EU Member state to identify operators of essential services with an establishment on their territory to achieve its goals. A critical factor in the NIS Directive's lack of efficiency is the broad criteria to identify these Operators of Essential Services (OES). The requirements are as follows:

- An entity provides a service that is essential for the maintenance of critical societal and economic activities
- The provision of that service depends on network and information systems
- An incident would have significant disruptive effects on the condition of that service.⁵³

The application of these criteria depends on the risk assessment of the national authority to the specific essential service. In other words, although transport is identified as a critical service for the EU, some member states could decide that some of their maritime infrastructures do not meet the criteria. Consequently, not all the ports and vessels in the EU are classified as critical infrastructure.

Another characteristic of the EU's maritime domain is the diversity of the national maritime competent authorities. Different entities, shown in the table below, have specific goals, regulatory frameworks, partners, and budgets, which creates further incoherence in the domain.

To respond to the growing threats posed by digitalization and the surge in cyberattacks, the EU Commission has submitted a proposal to replace the NIS Directive, strengthen the security requirements, and introduce more stringent supervisory measures and stricter enforcement requirements, including integrated sanctions across the European Union.⁵⁴ By adding many new sectors to the list of essential services, NIS 2 will address the security of supply chains and harmonize the reporting obligations.

⁵² ENISA, <https://www.enisa.europa.eu>.

⁵³ "NIS Directive – Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016."

⁵⁴ European Parliament, "The NIS2 Directive: A High Common Level of Cybersecurity in the EU," EU Legislation in Progress, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI\(2021\)689333_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf).

Table 2. EU National Competent Authorities.⁵⁵

Country	Competent Authority
Belgium	Federal Mobility Minister (Federal Public Service Mobility)
Croatia	Ministry of the Sea, Transport, and infrastructure
Czechia	National Cyber and Information Security Agency (NCISA)
Bulgaria	Ministry of Transport
Denmark	The Danish Transport, Construction, and Housing Authority
Estonia	Information System Authority (RIA)
Finland	Finnish Transport and Communications Agency Traficom
France	National Cybersecurity Agency ANSSI
Germany	Federal Office for Information Security (BSI)
Greece	National Cyber Security Authority (General Secretariat of Digital Policy - Ministry of Digital Policy, Telecommunications, and Media)
Hungary	National Directorate General for Disaster Management
Ireland	National Cyber Security Centre (NCSC)
Latvia	Ministry of Transport
Lithuania	Ministry of National Defence
Luxembourg	Institut Luxembourgeois de Régulation
Malta	Malta Critical Infrastructure Protection Unit (CIP)
Netherlands	Ministry of Infrastructure and Water Management
Poland	Ministry of Marine Economy and Inland Navigation
Portugal	National Cyber Security Centre Portugal
Romania	CERT-RO
Slovakia	Ministry of Transport and Construction of the Slovak Republic
Slovenia	Information Security Administration
Spain	Secretary of State for Security, -Ministry of Interior-, through the National Center for the Protection of Infrastructures and Cybersecurity (CNPIC)
Sweden	Swedish Transport Agency

⁵⁵ ENISA, “National Competent Authorities for the Water transport subsector,” <https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/nis-visualtool>.

NIS 2 has the following main objectives:

- Increase the level of cyber resilience of EU country services by putting in place rules that all public and private entities responsible for those services are required to take.
- Reduce inconsistencies in resilience across the internal market in the important service sectors by further aligning the security and incident reporting requirements and the governing national supervision and enforcement.
- Improve the level of collective situational awareness and the collective capability to prepare and respond by taking measures to increase trust between competent authorities. Share more information and set rules and procedures in the event of a large-scale incident or crisis.⁵⁶
- Improve the way the Member States draw up lists of operators of essential services by suggesting a standard set of criteria.

The backbone of protection and cyber resilience is set up around the European NIS cooperation groups' taxonomy of large-scale cyber incidents,⁵⁷ which defines all the potential malicious acts and further links them to the relevant EU political crisis response regulations. Other norms used to mitigate the risks and threats to the European maritime industry include the European Program for Critical Infrastructure Protection (EPCIP)⁵⁸ and the Directive on the Identification and Designation of European Critical Infrastructures.⁵⁹ Recently, the Proposal for a Directive on the resilience of essential entities has provided a more focused approach to critical infrastructure protection.⁶⁰

Specific maritime cybersecurity regulatory means are built around the EU's Maritime Security Strategy (EUMSS).⁶¹ This strategy identifies the marine security risks and threats of "*terrorism and other intentional unlawful acts at sea and in ports against ships, cargo, crew and passengers, ports and port facilities and*

⁵⁶ ENISA, <https://www.enisa.europa.eu>.

⁵⁷ The NIS cooperation group consists of representatives of EU member states, ENISA and the European Commission. It was established on the basis of Article 11 of the NIS Directive.

⁵⁸ European Programme for Critical Infrastructure Protection.

⁵⁹ "Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance)," Document 32008L0114, *EUR-Lex* December 23, 2008, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008L0114>.

⁶⁰ "Proposal for a Directive of the European Parliament and of the Council on the Resilience of Critical Entities," Document 52020PC0829, *EUR-Lex*, December 16, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:829:FIN>.

⁶¹ Council of the European Union, "Maritime Security Strategy," June 26, 2018, https://ec.europa.eu/oceans-and-fisheries/ocean/blue-economy/other-sectors/maritime-security-strategy_en.

*critical maritime and energy infrastructure, including cyberattacks.*⁶² EUMSS was adopted in 2014 and revised in 2018 as a shared and comprehensive tool to identify, prevent and respond to any challenge that affects the security of European people, activities, and assets in the maritime ecosystem. The revision of the EUMSS, as adopted by the General Affairs Council on June 26, 2018, aims at a more focused reporting process to enhance awareness and better follow-up to the strategy.

To implement the regulatory framework, the EU has set up specialized entities such as the European Union Agency for Cybersecurity (ENISA),⁶³ The European Cyber Crime Centre (EC3)⁶⁴ at Europol, and the Computer Emergency Response Team (CERT-EU).⁶⁵ The Directorate General for Mobility and Transport (DG MOVE) and the European Maritime Safety Agency (EMSA) perform general control over the national authorities in implementing the requirements. Moreover, the EU has launched initiatives to increase cybersecurity in various critical sectors. In particular, the Information Sharing and Analysis Centers (ISAC)⁶⁶ are intended to be trusted entities to foster information sharing and good practices about physical and cyber threats and their mitigation. However, currently, the EU lags in creating ISACs for the maritime domain.

An essential program for the EU countries was presented to the Member States in March 2021. “The Digital Compass 2030”⁶⁷ aims to implement specific procedures to enhance the EU’s digital transformation, improve its digital sovereignty and policies, and address vulnerabilities and threats. The program should support digitalization and increase sharing in the maritime domain by implementing state-of-the-art cybersecurity measures. The “Digital Compass 2030” is based on four key points:

- The digital empowerment of the population
- The enhancement of digital infrastructures connectivity and performance
- The digital transformation of businesses
- The digitalization of public services.⁶⁸

⁶² Council of the European Union, “Maritime Security Strategy.”

⁶³ ENISA, <https://www.enisa.europa.eu>.

⁶⁴ “European Cybercrime Centre – EC3: Combating Crime in a Digital Age,” *Europol*, updated March 1, 2022, <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3>.

⁶⁵ “CERT-EU – The Computer Emergency Response Team for the EU institutions, bodies and agencies,” <https://cert.europa.eu/>.

⁶⁶ “Information Sharing and Analysis Centers (ISACs),” <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing>.

⁶⁷ “2030 Digital Compass: The European Way for the Digital Decade,” *EU4Digital*, March 9, 2021, <https://eufordigital.eu/library/2030-digital-compass-the-european-way-for-the-digital-decade/>.

⁶⁸ “2030 Digital Compass.”

Fundamentally, the “Digital Compass 2030” is a clear demonstration of the EU’s ambitions to implement additional cybersecurity policies and strategies and provide other tools to improve digitalization and the EU’s economic and societal metrics.

The major challenge for the Member States is implementing the EU regulations. Currently, most Member States do not possess the technical capabilities and capacities to monitor the maritime critical information infrastructure, nor have they implemented specific rules to protect their relevant essential services. Other deficiencies are the lack of effective platforms and venues to share best practices and strengthen the collaboration between the Member States and their international counterparts, such as public-private partnerships.⁶⁹

Another major obstacle in pursuing an efficient level of cyber resilience in the EU is applying penalties to those entities that are not compliant with the requirements. However, because of the lack of national will across the Member States, the penalties are, in most cases, irrelevant and inapplicable.⁷⁰

Overview of the US Maritime Cybersecurity Framework

US maritime cybersecurity framework does not differ fundamentally from the EU’s approach. The US National Maritime Cybersecurity plan regulates maritime cybersecurity. Its principles are:

- Freedom of the seas
- Facilitation and defense of commerce to ensure the uninterrupted flow of shipping
- Facilitation of the movement of desirable goods and people across borders while screening out dangerous people and materials.⁷¹

The plan unifies maritime cybersecurity resources, stakeholders, and initiatives, mitigating current threats, vulnerabilities, and complements.⁷²

Other US policies on cyber measures for the maritime domain are the Navigation and Vessel Inspection Circular No. 01-20 “Guidelines for addressing a cyber risk at maritime transportation security act” (MTSA)⁷³ and a Commercial

⁶⁹ Cecilia Gondard and Enrique Guerrero Salom, “The Problem with Public-Private Partnerships and the Role of the EU,” *Eurodad*, December 4, 2018, <https://www.eurodad.org/PPPs-EU>.

⁷⁰ This issue is addressed in the NIS2.

⁷¹ “National Maritime Cybersecurity Plan to the National Strategy for Maritime Security” (The White House, December 2020), <https://www.hsdl.org/?view&did=848704>.

⁷² “National Maritime Cybersecurity Plan to the National Strategy for Maritime Security.”

⁷³ U.S. Coast Guard, “Navigation and Vessel Inspection Circular (NVIC) No. 01-20 – Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities,” February 26, 2020, <https://www.dco.uscg.mil/Our-Organization/NVIC/Year/2020/>.

Vessel Compliance Work Instruction – CVC-WI-018(1).⁷⁴ These policies set deadlines for vessels and waterfront facilities to incorporate cyber protection activities into their security assessments and plans.

A critical challenge for the United States Coast Guard, the national maritime authority of the United States, is creating specific policies and unilaterally assessing the cybersecurity infrastructure’s strength and “hardness.” This is related to the lack of sharing and reporting, as well as a lack of capacities and procedures to evaluate the level of vulnerability.

A significant challenge for the international and regional maritime cybersecurity frameworks is how to minimize the threats to the ports and the cargo deriving from vessels using “flags of convenience” (FOC). These flag registries do not have specific nationality requirements for the shipping companies that use their flag.⁷⁵ According to UNCTAD, almost seventy-three percent of ships are flagged in a country different than the vessels’ owner.⁷⁶ The problem is that despite having ratified several international maritime and labor conventions, FOCs often lack the resources or the will to enforce international maritime security and cybersecurity regulations effectively. Hence, they create a critical vulnerability to the whole maritime transportation system.

To summarize, the main challenges to the efficiency of the current regulatory framework are connected to the following key factors:

- Lack of harmonization and standardization between the existing frameworks
- Lack of will to enforce implementation of effective cybersecurity tools and sanctions in the case of non-compliance
- Lack of cyber awareness.

Examples

Fortunately, despite all the difficulties and challenges, some examples show that cyber resilience and cyber awareness are possible. The Norwegian Maritime Authority has warned ship owners and shipping companies that hackers have been using social media such as LinkedIn, Facebook Messenger, and WhatsApp to install malware. They issued specific recommendations to the ships and succeeded in reducing the potential impact of cyberattacks.⁷⁷

⁷⁴ USCG Office of Commercial Vessel Compliance (CG-CVC), “Commercial Vessel Compliance Work Instruction – CVC-WI-018(1)2020,” September 1, 2020, [www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/CG-CVC/CVC_MMS/CVC-WI-018\(1\).pdf](http://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/CG-CVC/CVC_MMS/CVC-WI-018(1).pdf).

⁷⁵ “Flags of Convenience,” *NGO Shipbreaking Platform*, <https://shipbreakingplatform.org/issues-of-interest/focs>.

⁷⁶ “Review of Maritime Transport,” *UNCTAD*, <https://unctad.org/topic/transport-and-trade-logistics/review-of-maritime-transport>.

⁷⁷ Norwegian Maritime Authority, <https://www.sdir.no/en/>.

The Shipowners Claims Bureau, Inc. created a novel way of training staff both onboard and at port terminals through a cartoon booklet entitled *Cyber Awareness*. Cartoon figures and humor explain how seafarers need to be conversant in cyberattack countermeasures, whether ransomware or phishing hacks.⁷⁸

Some EU Member States have embedded cyber awareness initiatives in their National Cybersecurity Strategies (NCSS). In Croatia, these initiatives cover electronic communication, critical information infrastructure, and cybercrime.⁷⁹ In the NCSS of the Czech Republic, it is covered in a separate chapter titled “Resilient Society 4.0.”⁸⁰ The Estonian NCSS implements specific means to raise awareness among citizens, prevent cybersecurity incidents, and notify citizens about possible threats.⁸¹ The primary objective of Poland’s Cybersecurity Strategy is to increase the level of resilience to cyber threats. It includes specific cybersecurity awareness programs.⁸²

ENISA’s cyber risk management tool for ports is another example of the beneficial effect of maritime collaboration. The tool allows port operators to conduct a cyber risk assessment with a four-phase approach following common risk management principles. Moreover, the operators identify security measures based on their priorities and assess their maturity in implementing these measures.⁸³

Regarding maritime sharing, the United States uses ISACs to share cyber threat information between various stakeholders. The US maritime sector has three additional ISACs (MPS-ISAO, Maritime ISAC, and the maritime transportation system ISAC).⁸⁴

Response

Since the digitalization and implementation of ICT into merchant shipping, vessels are challenged by cyber-related risks and threats. The merchant maritime

⁷⁸ Shipowners Claims Bureau, Inc., “Shipboard Safety Cartoon,” https://www.american-club.com/files/files/Shipboard_Safety.pdf.

⁷⁹ “The National Cybersecurity Strategy of the Republic of Croatia,” Zagreb, October 7, 2015 (Official Gazette No.108/2015), [https://www.uvns.hr/UserDocImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20\(2015\).pdf](https://www.uvns.hr/UserDocImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf).

⁸⁰ “Czech Republic Cybersecurity,” *International Trade Administration*, accessed May 13, 2021, <https://www.trade.gov/market-intelligence/czech-republic-cybersecurity>.

⁸¹ Ministry of Economic Affairs and Communications, *Cybersecurity Strategy, Republic of Estonia 2019-2022*, <https://www.mkm.ee/media/703/download>.

⁸² Waldemar Kitler, “The Cybersecurity Strategy of the Republic of Poland,” in *Cybersecurity in Poland*, ed. Katarzyna Chałubińska-Jentkiewicz, Filip Radoniewicz, and Tadeusz Zieliński (Cham: Springer, 2022), https://doi.org/10.1007/978-3-030-78551-2_9.

⁸³ “Cyber Risk Management for Ports,” *ENISA*, <https://www.enisa.europa.eu/cyber-risk-management-for-ports#/>.

⁸⁴ Jaikumar Vijayan, “What is an ISAC or ISAO? How These Cyber Threat Information Sharing Organizations Improve Security,” *CSO*, July 26, 2021, www.csoonline.com/article/3406505/what-is-an-isac-or-isao-how-these-cyber-threat-information-sharing-organizations-improve-security.html.

shipping environment is currently occupied by a variety of stakeholders and controlled by many regulatory entities, each using different norms. As a result of the lack of cyber awareness and state-of-the-art technical capabilities to monitor the vessel's information infrastructure, and because the existing norms are broad or not compulsory, maritime shipping is vulnerable to a cyberattack which could cause considerable damage.

The first and most important program should be focused on improving maritime threat sharing in the maritime domain. This could be accomplished by utilizing Information Sharing and Analysis Centers (ISACs) and promoting public-private partnerships. The second program should enhance cyber awareness in the whole maritime domain. This could be accomplished by organizing specific exercises, seminars, and conferences for the whole-of-maritime domain stakeholders. Moreover, training and certifications can be included and conducted throughout the year by government authorities that regulate and standardize the process. Both initiatives are essential elements of the EU NIS 2 Directive.⁸⁵

The third program should be dedicated to standardizing the existing legal framework. This could be accomplished by implementing a Global Maritime Cybersecurity Code, which would be easier to monitor and enforce. Moreover, a Global Code would harmonize the existing best practice in cybersecurity standards. As these standards already have international acceptance, compliance should meet less resistance from the ship owners and the national authorities. A Maritime Cybersecurity Code should have both mandatory and voluntary components. The mandatory section should be focused on ensuring the essential services of the ships. The voluntary section should cover the ways of implementing additional security measures. A sub-program should cover the FOC's accreditation and certification by implementing additional compulsory requirements to their information infrastructure. Moreover, the Maritime Cyber Code should have specific guidelines and procedures to attribute and further sanction the perpetrators of a cyberattack.

The fourth program should set up early detection capabilities for disruptive cyber events. Early detection could take many possible forms, including monitoring networks and data flows. On the operational level, this program should also include secured capacities for sharing between parties and effective means to guarantee the business continuity of the vessel. Cyber resilience should include clear plans for alternate communication channels, alternate informational databases fully independent from daily systems, and alternate tools and systems onboard vessels to guarantee that essential vessel services run continuously if the systems are breached. This program could be accomplished via EU and US-specific programs and funds.

The fifth program should counter the lack of skills in detecting a cybersecurity attack. The training should ensure that everyone can detect abnormal system behaviors and report them in a specific order. Moreover, the crew must be

⁸⁵ European Parliament, "The NIS2 Directive."

trained to follow strict cyber hygiene rules, including sophisticated authentication methods, limited access to resources, and verification of portable memory.

Finally, the last program should be focused on the recovery and reconstruction of the capabilities after a cyber incident. This could include specific exercises and training to restore essential vessel services, data restoration, incident response, and digital forensic activities. An essential aspect of this program should be based on the compensation of “the victims,” whether through liability insurance or government payments. Adequate compensation reduces societal risks and damages and contributes to the economy’s recovery, social stability, and trust in institutions.

Conclusion

In conclusion, the maritime cyber domain is a Titanic heading towards an iceberg. Without proper foresight and the ability of leaders in the maritime community to address its emerging vulnerabilities, it will only be a matter of time before a maritime cyberattack catastrophically affects the global maritime transport system. Although the research has identified that different entities have recognized threats to the shipping cybersecurity system in the specific norms and policies, the examination revealed that global cyber resilience had been affected lightly. In this regard, the international maritime community, supported by the regional and national maritime authorities, should execute a comprehensive program focusing on enhancing cyber awareness and harmonizing the existing regulatory framework to counter the threat. The success of such a program depends on all maritime community actors actively decreasing their cyber vulnerabilities and countering the respective risks and threats. Only then can the iceberg be avoided.

Disclaimer

The views expressed are solely those of the author and do not represent official views of the PFP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium’s editors.

About the Author

Yavor Todorov is a Marshall Center Alumni Scholar, a senior Expert at the State Agency for National Security /DANS/ of Bulgaria, and leads a unit in the Cybersecurity Department. Mr. Todorov has 20 years of experience in Bulgarian security services and has held various positions, including in the area of counterterrorism, counterintelligence, and cybersecurity, for the past eight years. Mr. Todorov is an ex-naval officer who has taken part in a number of multinational exercises aimed at strengthening security in the Black Sea region. He is a member of the Horizontal Working Party on Cyber Issues at the Council of the EU and drafted the National Cybersecurity Act and the related regulations. Currently, his team is executing vulnerability assessments on the national critical information infrastructure. In addition, he works closely with Bulgaria's partnering law enforcement agencies and services. Besides English, he speaks Italian and Russian languages. He holds an MSc degree in Telecommunications and Port Management from the Bulgarian Naval Academy and an MA in Strategic Studies from National Defense University, Washington DC. He is currently finishing his dissertation on Maritime Cybersecurity.



Security Threats of Radicalism through Social Media amid Covid-19 Pandemic: Indonesia's Perspective

Aththariq Rizki and Fauzia Gustarina Cempaka Timur

Asymmetric Warfare Study Program, Indonesia Defense University.

Abstract: The Covid-19 pandemic has brought so many uncertainties for society. People are compelled to adapt to the “new normal” in every aspect of their lives. The government of Indonesia introduced new policies to limit the movement of people through the Policy and the Work From Home (WFH) work system. As a result, large-scale social restrictions relied on the Internet, thus posing higher security risks. Even though the use of social media to spread radicalism is no longer considered novel, the pandemic has revamped social media into a more convenient platform for radicals and extremists as more people are engaged on a daily basis. By using qualitative methods, this study aims to analyze how the spread of radicalism through social media has become a tangible threat to Indonesia during the times of pandemic and the government's response strategy. This study found that the number of social media users in Indonesia peaked at 51.5 % since the start of the pandemic, most of which came from productive age groups. This study concluded that the pandemic had extended recruitment and radicalization through social media by reaching out to more people and spreading diverse narratives and hoaxes. In order to face those threats, Indonesia's government uses a strategy of combating such narratives, increasing digital literacy, and blocking content and accounts to minimize the echo of radicalization on social media.

Keywords: Covid-19, radicalism threat, social media, Indonesia

Introduction

The development of information and communication technologies is increasing rapidly. Technology is essentially made to assist and facilitate human activities.

Still, sometimes it is misused as a crime tool, especially during the COVID-19 pandemic, where individuals widely use technology to help them fulfill their lives, from formal work to daily activities.

Citing the International Telecommunication Union (ITU) report, the number of world internet users in 2018 increased to 3.9 billion, i.e., half of the world's population. The number of internet users has also increased significantly in Indonesia. According to the 2020 APJII survey results, the number of internet users in Indonesia was 171.1 million, an increase of 27.9 million from the previous year when it was only 143.2 million. In the last survey during 2019-2020 (Q2), it was found that internet user penetration in Indonesia had reached 196.71 million users. Hence, 73.1% of Indonesian people currently use the Internet.

Between 2019 and 2020, Internet use in Indonesia increased further. This increase was related to the spread of COVID-19, which also affected Indonesia. Reporting from *VOI* (Voice of Indonesia),¹ the APJII chairperson explained that the rise in the number of Internet users in Indonesia was due to the online learning and work-from-home policies due to the COVID-19 pandemic since March 2019. With so many activities being carried out online at home, Internet usage will also increase.

The COVID-19 pandemic has forced the Indonesian government to issue a policy of large-scale social restrictions. According to the Coordinating Ministry for Human Development and Culture,² "large-scale social restrictions" are restrictions on certain activities of residents in an area suspected of being infected with the SARS-CoV-2 virus. This policy aims to prevent the spread of COVID-19 by limiting community activities, including work activities. Every activity carried out by the community must also comply with 3M health protocols (wearing masks, washing hands, and maintaining distance). Based on APJII data,³ during the Covid-19 pandemic, as many as 51.5% of Indonesians actively use the Internet to access social media.

With the widespread use of social media during the COVID-19 pandemic, there have been numerous threats and concerns about using social media for criminal purposes and other malicious activities. One threat involves several parties exploiting social media to spread radicalism. The Head of the National Counter-Terrorism Agency (BNPT), Boy Rafli Amar,⁴ confirmed that radicalism spreads

¹ Tachta Citra Elfira and Aditya Fajar Indrawan, "APJII: Pandemi COVID-19 Buat Pengguna Internet di Indonesia Meningkatkan Hampir 200 Juta [APJII: The COVID-19 Pandemic Makes Internet Users in Indonesia Increase by Nearly 200 Million]," *VOI*, November 10, 2020, <https://voi.id/teknologi/19331/apjii-pandemi-Covid-19-buat-pengguna-internet-di-indonesia-meningkat-hampir-200-juta>.

² "Apa itu PSBB [What is PSBB]," *Kemenko PMK*, February 18, 2020, <https://www.kemenkopmk.go.id/apa-itu-psbb>.

³ Asosiasi Penyelenggara Jasa Internet Indonesia, "Laporan Survei Internet APJII 2019-2020 [Q2] [APJII Internet Survey Report 2019-2020]," December 23, 2020, <https://apjii.or.id/survei>.

⁴ Sania Mashabi, "Kepala BNPT: Penyebar Paham Radikalisme Manfaatkan Media Sosial [Head of BNPT: Spreaders of Radicalism Take Advantage of Social Media]," *Kompas*,

not only face-to-face. Currently, radicals are disseminating intolerant radical ideas through social media. Radical parties use the existing channels on their social media accounts to spread their extreme views. According to him, social media became one of the most effective means to reach the younger generation and incite radicalism during the pandemic. The main target group is teenagers aged 17 to 24 years. At this age, they are still young, energetic, and unstable about their identity.

Sunarto's research⁵ reveals that advances in information technology generate threats to the integrity of the life of the nation and the state. One of them is the ease of access to the Internet and social media, which makes it easier for people to receive information about radicalism, bomb-making, and crimes. Low literacy levels may facilitate radicalization through the internalization of values during the interaction with online media in the lack of a well-integrated family.⁶ However, the secondary social environment, where a person interacts socially in the neighborhood and the educational environment, may counter radicalization by attitudes of tolerance to diversity and difference so that he or she is not easily influenced by content with radical nuances.⁷

Several scholars agree with Sunarto and highlight that radicalization is now widespread in Indonesia. Therefore the government needs a suitable counter-radicalization communication strategy, which may specifically utilize social media.⁸ Ghifari⁹ has also found that, currently, the spread of radicalism in society on social media has contributed significantly to the dissemination of radicalism, where social media became a propaganda medium to carry out intolerant actions, such as recruitment and training events, education, member network de-

July 3, 2020, <https://nasional.kompas.com/read/2020/07/03/15343511/kepala-bnpt-penyebar-paham-radikalisme-manfaatkan-media-sosial?page=all>.

⁵ Andang Sunarto, "Dampak Media Sosial Terhadap Paham Radikalisme [The Impact of Social Media on Radicalism]," *Nuansa: Jurnal Studi Islam dan Kemasyarakatan* 10, no. 2 (December 2017): 126-131, <http://dx.doi.org/10.29300/nuansa.v10i2.647>.

⁶ Widodo Agus Setianto, "Literasi Konten Radikal di Media Online [Radical Content Literacy in Online Media]," *Jurnal Ilmu Komunikasi* 16, no. 1 (January-April 2018): 75-88, <https://doi.org/10.31315/jik.v16i1.2684>.

⁷ Surryanto D. Waluyo, Fauzia Gustarina Cempaka Timur, and Ningsih Susilawati, "Pengajaran Nilai Bela Negara Melalui Pendidikan Kewarganegaraan Sebagai Upaya Cegah Dini Terhadap Radikalisme [Teaching the Value of State Defense Through Citizenship Education as an Effort to Prevent Early Against Radicalism]," *Bhineka Tunggal Ika: Kajian Teori dan Praktik Pendidikan PKN* 8, no.1 (May 2021): 10-20, <https://ejournal.unsri.ac.id/index.php/jbti/article/view/12125/pdf>.

⁸ Ratna Puspita, "Kontra-Radikalisasi Pada Media Sosial Dalam Perspektif Komunikasi [Counter-Radicalization of Social Media in a Communication Perspective]," *Jurnal Komunikasi Universitas Garut: Hasil Pemikiran dan Penelitian* 6, no. 2 (October 2020): 509-529, <https://journal.uniga.ac.id/index.php/JK/article/view/785>.

⁹ Iman Fauzi Ghifari, "Radikalisme di Internet [Radicalism on the Internet]," *Religious: Jurnal Agama dan Lintas Budaya* 1, no. 2 (March 2017): 123-134, <https://journal.uinsgd.ac.id/index.php/Religious/article/view/1391>.

velopment to spread acts of terror and suicide bombings in Indonesia. Zamzamy¹⁰ added that the advancement of internet media allowed radicalism groups to recruit, propagate, and spread ideology. If, in the conventional method of spreading radicalism, it is necessary to meet with an ideology carrier, then this method is now available online. Radicalization is a process of seeking, discovering, adopting, and developing beliefs and extremes. The existence of online media is an instrument that has the potential to accelerate the radicalization process. From Aisy and colleagues,¹¹ we know that to deal with this, the government has increased cyber patrols to prevent the dissemination of content containing radicalism. Aside from that, the Ministry of Communication and Informatics strictly supervises content disseminated through social media applications, which has affected recruitment patterns and the spread of radicalism.¹²

Moreover, Handoko and Susanto¹³ elaborate that the role played by the Ministry of Communication and Informatics in preventing radicalism is already taken where they continue to educate the public about the dangers of radicalism and continue to counter every radicalism-related content through social media by sharing positive and peaceful narrative content. Interactions that occur on social media can be seen through the number of likes, shares, and comments. This number of interactions determines the reach of other social media users. The mention of a radicalism-related word on social media is not only related to religious issues. Other concerns associated with radicalism are elections, politics, government, crime, and other social issues.¹⁴

Fanindy and Mupida,¹⁵ through their research, also explain the results of social media as the first option for the younger generation in seeking instant infor-

¹⁰ Ahmad Zamzamy, "Menyoal Radikalisme di Media Digital [Questioning Radicalism in Digital Media]," *Dakwatuna: Jurnal Dakwah dan Komunikasi Islam* 5, no. 1 (February 2019): 13-29, <https://doi.org/10.36835/dakwatuna.v5i1.318>.

¹¹ Bilqis Rihadatul Aisy et al., "Penegakan Kontra Radikalisasi Melalui Media Sosial Oleh Pemerintah Dalam Menangkal Radikalisme [Enforcement of Counter-Radicalization Through Social Media by the Government in Countering Radicalism]," *Jurnal Hukum Magnum Opus* 2, no. 1 (February 2019): 1-8, <https://doi.org/10.30996/jhmo.v2i2.2174>.

¹² Achmad Sulfikar, "Swa-radikalisasi Melalui Media Sosial di Indonesia [Self-radicalization Through Social Media in Indonesia]," *Jurnal Jurnalisa* 4, no. 1 (May 2018): 76-89, <https://doi.org/10.24252/jurnalisa.v4i1.5622>.

¹³ Jefri Handoko and Eko Harry Susanto, "Humas Kominfo Dalam Mencegah Bahaya Radikalisme Di Media Sosial [Kominfo Public Relations in Preventing the Danger of Radicalism in Social Media]," *Jurnal Prologia* 3, no. 1 (July 2019): 147-153, <https://doi.org/10.24912/pr.v3i1.6232>.

¹⁴ Abdul Wahid, Nia Ashton Destitry, and Fariza Yuniar Rakhmawati, "Radikalisme di Media Sosial: Penyebutan dan Konteks Sosial Penggunaannya [Radicalism in Social Media: Mention and Social Context of Its Use]," *Jurnal InterAct* 9, no. 1 (2020): 60-70, <https://doi.org/10.25170/interact.v9i1.1711>.

¹⁵ M. Nanda Fanindy and Siti Mupida, "Pergeseran Literasi pada Generasi Milenial Akibat Penyebaran Radikalisme di Media Sosial [Literacy Shift in Millennial Generation Due

mation so that they are easily exposed to radicalism content. The young generation is easily exposed to radicalism because they are in the process of finding their identity; thus, they will be influenced easily by what they read. Also, because they are familiar with how social media may grant them diverse information instantly, extremist groups use the same logic. Initially, they spread radicalism in the name of religion to uphold the ideology of the caliphate and reject the democratic system through writings, books, and magazines and uploading them to social media networks considered more effective.

So looking at the prior arguments, during the COVID-19 pandemic, health protocols and government policies have limited people's physical movements, which led to increased activity on the Internet, especially on social media. Of course, this is a potential for the growing threat of radicalism on social media. Therefore, below we analyze in more detail the threat perception of radicalism via social media in Indonesia during the COVID-19 pandemic.

Method

In writing this article, the authors use a qualitative research method with a literature review approach. According to Creswell,¹⁶ a literature review is a research approach based on non-numeric data, which can be in the form of writing and images, and filtering of the data is carried out to make interpretations of the literature review. This research study has been conducted through literature sources such as journals, books, theses, research reports, and scientific articles with valid and reliable sources.

Finding and Discussion

Use of Social Media during the COVID-19 Pandemic in Indonesia

The Digital Trends Report, a survey conducted by Facebook with YouGov, shows that more than 140 million Indonesians joined social media groups that were active during the COVID-19 pandemic. Currently, Indonesia's population is 267.7 million people. Ninety-five percent of the respondents claimed to provide support, both moral assistance and household needs, to community members via social media during the COVID-19 pandemic. As many as 54 percent of respondents received moral support from their friends in the Facebook group, and another 55 percent provided moral support via social media. More than half of the social media community thrives on digital platforms. A total of 67 respondents said the community had become increasingly important during the COVID-19

to the Spread of Radicalism on Social Media],” *Millah: Jurnal Studi Agama* 20, no. 2 (February 2021): 195-222, <https://doi.org/10.20885/millah.vol20.iss2.art1>.

¹⁶ John W. Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, 2nd ed. (Thousand Oaks, California: Sage Publishing, 2003).

pandemic. Furthermore, as reported by *Kompas*¹⁷ on the basis of the latest report from the marketing agency “We Are Social” and social media management platform Hootsuite, more than half of the population in Indonesia was “literate,” i.e., actively using social media in January 2021 during the COVID-19 pandemic. The report entitled “Digital 2021: The Latest Insights into The State of Digital” claimed that out of a total of 274.9 million people in Indonesia, 170 million had used social media. Thus, the penetration rate is around 61.8 percent.

As of January 2021, active social media users in Indonesia have grown by 10 million, or around 6.3 percent, compared to January 2020. At the same time, internet users in Indonesia have also increased by 27 million or 15.5 percent, so currently, internet users in Indonesia are 202.6 million. Rohmah’s research¹⁸ shows that from 50 random samples on Instagram, 80% of people agreed that social media could be used as a medium of general information, and 93% agreed with social media as a medium for COVID-19 information. Furthermore, Rohmah¹⁹ also explained that 80% of his research respondents agreed that social media could be an escape from all problems. For individuals isolated during the COVID-19 pandemic, social media has become a source of entertainment and psychological relief.

This increase in the use of social media is in line with the convenience provided by social media.²⁰ Five aspects of social media’s superior characteristics make it a stronger choice than traditional media. Among its advantages are:

1. *Accessibility*: social media is easily accessible since it requires a small fee or is accessible at no cost
2. *Speed*: information and content on social media will be immediately available to everyone on networks, forums, and communities when the content or information is published
3. *Interactivity*: social media has the ability to accommodate two or more communication channels

¹⁷ Conney Stephanie, “Riset Ungkap Lebih dari Separuh Penduduk Indonesia ‘Melek’ Media Sosial [Research Reveals That More Than Half of Indonesia’s Population Is ‘Literate’ on Social Media],” *Kompas*, February 24, 2021, <https://tekno.kompas.com/read/2021/02/24/08050027/riset-ungkap-lebih-dari-separuh-penduduk-indonesia-melek-media-sosial>.

¹⁸ Nurliya Ni’matul Rohmah, “Media Sosial Sebagai Media Alternatif Manfaat dan Pemuas Kebutuhan Informasi Masa Pandemi Global Covid-19 (Kajian Analisis Teori Uses And Gratification) [Social Media as an Alternative Media Benefit and Satisfying Information Needs During the Global Covid 19 Pandemic (Analysis Study of Uses and Gratification Theory)], *Al-I’lam: Jurnal Komunikasi dan Penyiaran Islam* 4, no. 1 (September 2020): 1-16, <https://journal.ummat.ac.id/index.php/jail/article/view/2957>.

¹⁹ Rohmah, “Media Sosial Sebagai Media Alternatif Manfaat dan Pemuas Kebutuhan Informasi Masa Pandemi Global Covid-19.”

²⁰ Varinder Taprial and Priya Kanwar, *Understanding Social Media* (London: Ventus Publishing ApS, 2012).

4. *Longevity*: information or content on social media can be accessed for a long time or even forever.
5. *Reach*: social media and the Internet offer an unlimited range of all available content.

Meanwhile, based on a survey conducted by GWI in the third quarter of 2020 in *Beritasatu*,²¹ Youtube is still the most popular social media in Indonesia. The number of YouTube users reached 94%, with ages 16 to 64 years. The second most popular social media in Indonesia is WhatsApp, followed by Instagram in the third position. In the report, Instagram rose to third place by displacing Facebook to fourth.

The Threat of Terrorism and Radicalism in Indonesia during the COVID-19 Pandemic

Aisy and coworkers²² explain that radicalism is the forerunner to the formation of terrorism. Radicalism is an attitude that wants change as a whole and is revolutionary in nature, with a fast tempo, and against existing values with violence and extreme actions. During the COVID-19 pandemic, radicalism and terrorist activities often occur in Indonesia. Even at the beginning of 2021, terrorist activities from radical groups are increasingly being carried out. There was a bomb terror attack in Makassar – a suicide bomber attacked the Makassar Cathedral Church, South Sulawesi. Police said the bombers were part of the radical group *Jamaah Ansharut Daulah (JAD)*. The National Police Chief, General Listyo, stated that the four people were partners of L and YSF in participating in the study at the Villa Mutiara Housing. The housing was the location in Makassar for the arrest of members of the JAD terrorist network.²³ Suspect ZA carried out a terror attack with an airsoft gun inside the National Police Headquarters. In his statement, the National Police Chief said that ZA managed to break into the Police Headquarters complex through the back door and then went to the police post near the front entrance and carried out an act of terror. Based on the police report, ZA had left the post but returned again and fired six shots.²⁴

²¹ Yudo Dahono, "Data: Ini Media Sosial Paling Populer di Indonesia 2020-2021 [Data: This is the Most Popular Social Media in Indonesia 2020-2021]," *Beritasatu.com*, February 15, 2021, <https://www.beritasatu.com/digital/733355/data-ini-media-sosial-paling-populer-di-indonesia-20202021>.

²² Aisy et al., "Penegakan Kontra Radikalisasi Melalui Media Sosial Oleh Pemerintah Dalam Menangkal Radikalisme."

²³ Tommy Kurnia, "4 Kasus Terorisme yang Terjadi di Dunia Selama Pandemi COVID-19 [4 Terrorism Cases That Happened in the World During the COVID-19 Pandemic]," *Liputan 6*, March 29, 2021, <https://www.liputan6.com/global/read/4518650/4-kasus-terorisme-yang-terjadi-di-dunia-selama-pandemi-covid-19>.

²⁴ Berita Utama, "Penembakan Mabes Polri: 'Terduga teroris berideologi ISIS', polisi ungkap identitas perempuan 25 tahun pelaku serangan [Police Headquarters shooting: 'Suspected terrorist with ISIS ideology', police reveal the identity of the 25-year-

In interviews with the Indonesia Intelligent Agency (2020), the National Police explained that during March – December 2020, it suspected 143 people were involved in terrorism and radicalism. The police revealed that of the 143 suspects, 97 were from the Jamaah Ansharut Daulah (JAD) group, 20 were from the Jamaah Islamiyah (JI), 12 were from the East Indonesia Mujahidin group (MIT), and 14 from the social media.

The rise of terror and radicalism activities carried out by radical groups cannot be separated from the factors that support the spread of radicalism and terrorism in Indonesia. This is in line with Fatkhuri's opinion,²⁵ which states that two supporting factors trigger the spread of radicalism and terrorism in Indonesia, namely, economic deprivation and political injustice. The first is related to the problem of economic deprivation. Reporting from Wijaya in BBC Indonesia,²⁶ the Central Statistics Agency (BPS) noted that the number of poor people in Indonesia increased by more than 2.7 million people due to the COVID-19 pandemic. It was noted that the number of poor people in Indonesia in September 2020 reached 27.55 million, which is equal to 10.19 percent of the total population, an increase of 2.76 million people compared to September 2019. This increase in the poverty rate cannot be separated from the mass layoffs carried out by several private companies affected by the restrictions imposed during the pandemic.

This is in line with previous research conducted by Fanindy and Mupida,²⁷ which concluded that poverty was one of the factors supporting the terrorism or radicalism movement in Indonesia, although this did not directly affect the spread of radicalism. However, poverty easily influences someone in supplying their needs. This enables an economical approach to tackle radicalism and religious extremism. With widespread poverty, many Indonesians are trying to get income and material support from many sources. Radical groups and terrorists can use this to spread radical ideas and recruit by providing material support.

Second, there are issues related to political injustice. Many terrorist and radical groups saw government policies during the pandemic as an opportunity to attack the government and influence the minds of the Indonesian people. The economic condition worsened due to the Covid-19 pandemic. The government

old woman who carried out the attack],” *BBC News*, March 31, 2021, www.bbc.com/indonesia/indonesia-56579674.

²⁵ Fatkhuri, “Faktor Pendukung Terbentuknya Radikalisme dan Terorisme di Indonesia [Factors Supporting the Formation of Radicalism and Terrorism in Indonesia],” *Jurnal Universitas Pembangunan Veteran Jakarta* (2017), https://www.researchgate.net/publication/318054171_FAKTOR_PENDUKUNG_TERBENTUKNYA_RADIKALISME_DAN_TERORISME_DI_INDONESIA.

²⁶ Callistasia Wijaya, “Dampak Covid-19: 2,7 juta orang masuk kategori miskin selama pandemi, pemulihan ekonomi ‘butuh waktu lama’ [Impact of Covid-19: 2.7 million people categorized as poor during the pandemic, economic recovery ‘takes a long time’],” February 17, 2021, <https://www.bbc.com/indonesia/indonesia-55992498>.

²⁷ Fanindy and Mupida, “Pergeseran Literasi pada Generasi Milenial Akibat Penyebaran Radikalisme di Media Sosial.”

policy was considered unfair and detrimental to small communities, especially for the workers. Yahya in Kompas²⁸ reported in October 2020 that the government and the Indonesian House of Representatives passed the Omnibus Law on Job Creation in a plenary meeting. However, this bill's ratification received much criticism from the Indonesian people. Many parties deplore the ratification of the Job Creation Bill. This bill is considered problematic and can potentially harm people, especially workers. Moreover, the ratification of the bill was carried out during the outbreak of the pandemic.

Waluyo and colleagues²⁹ have explained this political injustice stating that the dissatisfaction of several community groups leads to the emergence of terrorist movements and acts of radicalism. This feeling of dissatisfaction prompts the formation of radical groups, which then leads to terrorism, intending to confront the government.

In addition, Chaidir³⁰ also explains that BNPT has tried to analyze four attitudes toward terrorism and radical groups during the Covid-19 pandemic, namely:

1. Terrorist and radical groups circulate the idea that the spread of COVID-19 is a punishment for infidels and oppose government policies to follow health protocols.
2. Terrorist and radical groups take advantage of the PSBB period to carry out propaganda on social media.
3. Terrorist and radical groups view the COVID-19 pandemic as the right time to carry out acts of terror.
4. Terrorist and radical groups take advantage of the COVID-19 pandemic period for capacity building, spreading their narratives and recruiting people online.

²⁸ Achmad Nasrudin Yahya, "Ramai-ramai Menolak UU Cipta Kerja dan Ancaman Nasional [Many Against the Law on Job Creation and National Threats]," *Kompas.com*, June 10, 2020, <https://nasional.kompas.com/read/2020/10/06/05545351/ramai-ramai-menolak-uu-cipta-kerja-dan-ancaman-mogok-kerja-nasional?page=all>.

²⁹ Waluyo, Timur, and Susilawati, "Pengajaran Nilai Bela Negara Melalui Pendidikan Kewarganegaraan Sebagai Upaya Cegah Dini Terhadap Radikalisme."

³⁰ Leski Rizkinaswara, "Pemblokiran dan Literasi jadi Langkah Kominfo Cegah Terorisme di Ruang Digital [Blocking and Literacy are steps for Kominfo to Prevent Terrorism in the Digital Space]," *Jakarta: Aptika Kominfo*, August 16, 2020, <https://aptika.kominfo.go.id/2020/08/pemblokiran-dan-literasi-jadi-langkah-kominfo-cegah-terorisme-di-ruang-digital/>.

The Threat of Radicalism via Social Media in Indonesia during the COVID-19 Pandemic

From Wahid's previous research,³¹ it is known that the mention of the word "radicalism" is often followed by the use of hashtags (#) associated with other words. Some popular hashtags related to the mention of radicalism are #radicalism, #indonesia, #pancasila, #indonesiapeace, #indonesiahebat, #tolerance, #bhinnekatunggalika, and others. Moreover, various uses of these hashtags appear along with important events at certain times. Ines von Behr and colleagues³² explain that there are five reasons why the Internet and social media have an important role in promoting radicalism, namely:

1. The Internet and social media create more opportunities
2. The Internet and social media act as "echo chambers"
3. The Internet and social media accelerate the radicalization process
4. The Internet and social media allow radicalization to occur without physical contact
5. The Internet and social media increase opportunities for self-radicalization.

According to Anthonius Malau, director of Information and Communications Application Control at the Communications and Informatics website (2020), acts of terrorism and the spread of radicalism and information during the Covid-19 pandemic were still high. Records from July 2017 to July 2020 show that 16,739 pieces of content (on social media and websites) related to terrorism and radicalism were successfully blocked.

Meanwhile, according to the Director of BNPT Protection, Herwan Chaidir, the Kominfo website³³ also recorded increased cases related to terrorism and radicalism. From January to June 2020, 84 terrorism suspects were prosecuted by the police. According to Chaidir,³⁴ the Covid-19 pandemic caused 2 million people to lose jobs and increased poverty. The data provided by the BNPT indicates efforts to tackle these terrorist and radical groups so that they do not use the pandemic to recruit members.

As for social media content that can be said to be radical content, according to the guidebook for preventing radicalism in the work environment of BUMN and private companies by BNPT (2020), it has been found that four indicators

³¹ Wahid, Destitry, and Rakhmawati, "Radikalisme di Media Sosial: Penyebutan dan Konteks Sosial Penggunaannya."

³² Ines von Behr, Anaïs Reding, Charlie Edwards, and Luke Gribbon, *Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism* (RAND Europe, 2013).

³³ Rizkinaswara, "Pemblokiran dan Literasi jadi Langkah Kominfo Cegah Terorisme di Ruang Digital."

³⁴ Rizkinaswara, "Pemblokiran dan Literasi jadi Langkah Kominfo Cegah Terorisme di Ruang Digital."

characterize a group or individual as radical: intolerance, fanaticism, exclusivism, and anarchism. Here are examples of anarchic content circulating during the COVID-19 pandemic on social media based on BNPT’s radical indicators:

Table 1. Radical Activities on Social Media during the Covid-19 Pandemic.

No.	Case	Category	Date
1	The raid on houses of worship in Cikarang	Intolerance	13-09-2020
2	Fanatical support for the radical FPI movement	Fanatism	30-12-2020
3	Rejection of the Gospel in Minangnese language	Exclusivism	10-06-2020
4	Instructions against the FPI Command 1 government	Anarchism	26-06-2020

Table 1 lists cases from 2020 illustrating each of the four categories of radicalism defined by BNPT: intolerance, fanaticism, exclusivism, and anarchism. From the report of *Kumparan.com*,³⁵ one example of intolerant actions during the COVID-19 pandemic was the viral video on social media of the raid on a Christian house of worship in Cikarang, West Java. Local residents raiding the church were considered to have violated large-scale social restrictions (PSBB).

Aside from the intolerance category, fanaticism action has also been found in the data obtained from *Warta Ekonomi*.³⁶ The news of freezing the Islamic Defenders Front (FPI) community organization through the hashtag #FPIterlarang became a trend on Indonesian Twitter. Many Indonesian netizens showed their support together with FPI fanatics who are still trying to support and defend FPI through social media. Members and supporters of FPI spread such tweets, which have been seen as fanaticism towards the organization they run and idolize.

In one example, a June 2020 news was spread exclusively via social media. A Minangkabau community group objected to the publication of the Bible in the Minangkabau language. This act of rejection was channeled via social media tweets or direct reports, claiming that this publication was considered controversial and against the customs and culture of the Minangkabau people. An ex-

³⁵ Anwar Saragih, “Intoleransi di Masa Pandemi [Intolerance during a Pandemic],” *Kumparan.com*, April 20, 2020, <https://kumparan.com/anwar-saragih/intoleransi-dimasapandemi-1tG7MN5ffb0>.

³⁶ “FPI Dibubarkan, Warganet Pro-Kontra! Ada yang Bilang, ‘FPI Tetap di Hati!’ [FPI Disbanded, Warganet Pros and Cons! Some Say, ‘FPI Remains in the Heart!’],” *Wartaekonomi*, December 30, 2020, <https://www.wartaekonomi.co.id/read320669/fpi-dibubarkan-warganet-pro-kontra-ada-yang-bilang-fpi-tetap-di-hati>.

ample of an anarchistic call to action via social media during the COVID-19 pandemic was a call for jihad to fight against the Trisila communist group in Indonesia. Quoted in *Fajar.co.id*,³⁷ the General Secretary of FPI Munarman issued the first Command Alert instruction inviting jihad resistance to communist groups in Indonesia. This was a response to the actions of the Trisila group after the alliance held a demonstration against the draft Pancasila Ideological Direction Law.

Conclusion

Social media has turned into an essential platform for information, entertainment, and communication with the community and other people during the pandemic. In 2020, the most used social media in Indonesia was Youtube, followed by WhatsApp and Instagram.

During the COVID-19 pandemic, the threat of radicalism has increased. There are two reasons why an increased number of society members have turned to radicalism during the Covid-19 pandemic. First, the problem of economic deprivation, which got worse during the pandemic, and second, the political injustice felt by society. Many people were dissatisfied with what was perceived as unfair treatment by governmental policies. Inefficiencies in handling Covid-19 in Indonesia are among the causes for the emergence of this feeling of dissatisfaction. As a result, several cases of radicalism in 2020 indicated intolerance, fanaticism, exclusivism, and anarchism.

Disclaimer

The views expressed are solely those of the 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.

About the Authors

Aththaariq Rizki is a student in the Asymmetric Warfare Study Program at Indonesia Defense University, Bogor. E-mail: erikatorik@gmail.com

Fauzia Gustarina Cempaka Timur is a Lecturer in the Asymmetric Warfare Study Program at Indonesia Defense University, Bogor. E-mail: fgccempaka@gmail.com

³⁷ Adi Mirsan, "Siaga 1, FPI Cs Serukan Jihad Qital Lawan Komunis [Alert 1, FPI Cs Calls for Qital Jihad Against Communists]," *Fajar.co.id*, June 26, 2020, <https://fajar.co.id/2020/06/26/siaga-1-fpi-pa-212-dan-gnpf-serukan-jihad-qital-lawan-komunis/>.



A Reciprocal Relation: How Taliban and the World See Each Other

Mirwais Balkhi

School of Foreign Service, Georgetown University, <https://sfs.georgetown.edu/>

Abstract: On August 15, 2021, the 20-year war against the Taliban, led by the US/NATO alliance and the Afghan National Defense and Security Forces, ended with a dramatic Taliban takeover of power in Afghanistan. For the second time, they announced an acting government in Kabul. The re-emergence of the Taliban in the political arena of Afghanistan necessitates an analysis of how the Taliban and the countries involved in the Afghanistan conflict view each other. What will be the nature of reciprocal relations between the Taliban and other concerned states? How does the Taliban view the different regions that have engaged in Afghanistan over the past 20 years? Moreover, how do various capitals perceive the Taliban, a question frequently asked by media and think tanks? While global actors have viewed the Taliban with different attitudes, how will they perceive them in the future? This article attempts to answer most of these questions.

Keywords: tribalism, politicized religion, linguistic nationalism, foreign relations.

Introduction

On August 15, 2021, the Taliban marked a turning point in the history of Afghanistan by seizing power for the second time and announcing an interim government in Kabul. Their first victory and the capture of Kabul led to a regime that lasted for five years (1996-2001). The dramatic overthrow of the US-backed government and the surprising takeover of power by the Taliban in 2021 has confronted all regional and international players with ambiguity as to whether they will recognize this acting regime in Kabul or oppose it. Even long-term supporters

of the Taliban, like Pakistan, China, Russia, Iran, Qatar, and Saudi Arabia, do not know what to do.

Traditionally, neither the Taliban nor the international players would have thought that power politics inside Afghanistan could shift so quickly. The Taliban leadership was perplexed about how a fully equipped and NATO/US-backed army could crumble without much effort. In just a few weeks, the Taliban emerged from hiding, attacked significant cities, and established themselves in Kabul. International NGOs, embassy staff, and US troops were still in Kabul, and even the so-called advanced intelligence was caught off guard. As a result, Kabul descended into a “state of nature,” with the sounds of gunshots from robbers echoing throughout the city – a result of the total collapse that occurred within a few hours.

The scenario in Afghanistan has left those engaged in the conflict from outside in a similar situation. Presidents, foreign ministers, representatives, parliaments, and opposition parties of countries involved in the Afghan conflict found themselves caught in an unprecedented crisis. Over three months have passed since the Taliban seized power, yet no one has been able to decide or dared to lead an initiative to define diplomatic relations towards the Taliban. The Taliban, still unclear about their security strategies, replaced the comparatively democratic government in Afghanistan overnight. Although the Taliban talked about granting national amnesty and defining a peaceful engagement with the world, it is hard to trust their words. What will happen to democratic values, likely to perish under the Taliban? Would they support an Islamist group, or will they insist on an inclusive government? What will happen to the ordinary people of Afghanistan facing a humanitarian disaster? These are the pressing questions that need to be addressed.

All the players involved in the Afghan conflict are analyzing the Taliban regime, both individually and collectively, to formulate their foreign policy outlines. Many expect the United States to take a lead role and provide a strategic roadmap to ease the ambiguity. However, the US role will likely be minimal.

Therefore, it is necessary to review the analyses of a variety of national and international experts. These analyses are expected to complement each other and provide insights from both insiders and outsiders, depending on how the world perceives Afghanistan. Implementing this approach, in the article, we will analyze the reciprocal relations between the Taliban and international players.

Who Are the Taliban?

The term “Taliban” comes from the plural Arabic/Persian word for “students,” which refers to religious madrasa students. The group is made up of rural youths living in remote areas of Afghanistan who lack modern education, skills, and interactions. They represent a conservative, radicalized, and tribal group that is unable to compete in the modern labor market. Due to their opposition to modernism and dissatisfaction with the Afghan government, as well as the sup-

port of the Pakistani Inter-Services Intelligence (ISI) and other regional intelligence agencies, they have gained power. The Taliban are used as strategic assets to maintain influence or counter hostile forces in Afghanistan, creating a reciprocal relationship between the group and these intelligence agencies. Therefore, it is essential to study the Taliban in the context of Afghanistan's ethnic politics and regional interventionism.

The emergence of the Taliban is one of the most significant events in Afghanistan's history, with their formation dating back to the Soviet military invasion of Afghanistan and the eventual defeat by the Mujahideen. When the Mujahideen leaders arrived in Kabul and formed the Islamic State of Afghanistan, presided over by Burhanuddin Rabbani, they dealt with regional allies and Pakistan when it came to state-to-state relations. This was not acceptable to the Pakistani military, who hoped for a weak puppet regime in Kabul to preserve Pakistan's supremacy in Afghanistan and provide the Pakistani government with open access to Central Asia. This expectation arose due to the power vacuum following the disintegration of the Soviet rule in Afghanistan. Taking advantage of the uncertain situation of ethnic clashes and power distribution problems in Kabul, Pakistan fueled its internal allies against the government in Kabul.

The Pakistanis were unable to establish a pro-Islamabad government in post-Soviet era Afghanistan and did not want to be involved in a prolonged war there. As a result, Pakistan did not receive international funds for legitimate fighting in Afghanistan. Therefore, they developed a new strategy to confront the Mujahideen regime in Kabul, aiming to replace the new leadership and seek more international support. They supported the deprived Pashtun leaders in southern Afghanistan, and in 1994, a small group called the Taliban, made up of students from religious schools (*Madrassas*), declared themselves to be in opposition to the government in Kabul and requested all civil war parties in Afghanistan to surrender to them.

However, some analysts believe that the Taliban emerged as an autonomous but small group in Kandahar in 1994, opposing the acts of the Mujahideen leaders. The Taliban argued that the Mujahideen fought for power and misused Islam to justify their actions. Feeling insulted and disrespected, they decided to end this corrupt cohort. But one might ask how this small group turned into such a large force. Did they benefit from the support of foreign actors and the involvement of countries such as Pakistan, the United States, and Saudi Arabia?¹ Despite being an Islamic movement, the group has frequently committed violent, felonious acts, including drug dealing and indiscriminate, brutal murder.

On the other hand, since the Taliban claimed to be Islamist, it has presented an illogical and violent picture of Islam to the world. Are these acts the outcome of the fundamentalists' religious teachings, or should the reason be searched in

¹ Peter Marsden, *The Taliban: War, Religion and the New Order in Afghanistan* (Palgrave Macmillan, 1998), 169.

the country's social, cultural, and ethnic context? The social circumstances of Afghanistan have paved the way for reactionary views coming from the Indian sub-continent and Saudi Arabia. The Taliban announced themselves to the nation with "the campaign against the problems caused by the Afghan Mujahideen for people" as their motto. They declared their aims to disarm the Mujahideen groups fighting in civil wars, stop the production, dealing, and trafficking of drugs, combat administrative corruption, and reduce social crimes. However, their ultimate aim has been to establish an Islamic government based on definite inflexible perceptions and interpretations of Islam.²

The Taliban's Three-Pillars Objectives

In international relations, it is commonly understood that a player's actions are influenced by their internal politics. Without comprehending the Taliban's significance and nature as a regional player, analyzing their relations with other countries will be challenging.

It should be noted that "the Taliban has no foreign policy," despite the common belief. Rather, one can examine the "foreign relations" of a movement based on their "set of beliefs." By using the concept of foreign policy, we may inadvertently overlook important facts. Foreign policy is a road for a state to follow its interests, and, unfortunately, in the case of Afghanistan, the Taliban emerged as a non-state actor with territorial ambitions.

The Taliban's attitude towards foreign relations and strategies has differed before and after they seized power in Afghanistan. Prior to taking power, their efforts were focused on finding regional and global supporters in their war against the US-led forces and their ally in Kabul. However, after seizing power, they shifted their focus to strengthening their position nationally and gaining support from their regional partners.

The nature of the Taliban movement comprises a combination of tribalism, language, and politicized religion, which form its three main pillars. With this in mind, it is possible to better understand the Taliban's relations with countries in the region and the world. Anyone who supports these three goals is considered a friend of the Taliban, while anyone who opposes them is viewed as an enemy. Therefore, the Taliban's actions within Afghanistan, based on the three pillars of Pashtunwali³ tribal codes, linguistic nationalism (primarily using the Pashtu language), and a politicized Deobandi interpretation of Islam influenced by a rejectionist understanding of anti-imperialism during the early 20th century and the

² Rohullah Shaikhzada, "An Assessment of the Security Challenges between 2001-2010," MA Dissertation (Isfahan, Iran: University of Isfahan, 2011), 71-76.

³ Pashtunwali refers to the traditional lifestyle and code of honor followed by the Pashtun people. It is commonly referred to as "the way of the Afghans" and is practiced by Pashtuns in the Pashtunistan regions of Afghanistan, Khyber Pakhtunkhwa, and Northern Balochistan, as defined by scholars. See Erinn Banting, *Afghanistan: The Land (Lands, Peoples & Cultures)* (Canada: Crabtree Publishing, 2003).

later Soviet invasion of Afghanistan, can reflect their actions towards the region and the world.

Therefore, countries such as Pakistan and Iran are unlikely to have a friendly relationship with the Taliban. While Iran may have been an ally of the Taliban in their pre-power days and during the US-led invasion, it cannot be considered a friend of the Taliban in all three dimensions. Iran's opposition to the Taliban's primary objectives has led to clashes of interest. First, Iran opposes the generalization of Pashtunwali. Second, the Iranian claims for a "cultural Iran," which covers Afghanistan and Central Asia in its eastern borders, oppose the Taliban's expansionist strategy to rule Afghanistan. Third, there is a clash of historical memories between the Taliban and Tehran, as the Hotaki dynasty, which ruled Isfahan (modern Iran) from 1722 to 1738, is the most anti-Iranian historical symbol.

Linguistically, Iran is also seen as a hindrance to the Taliban's linguistic nationalism. Pashtun nationalism, which is reflected more in language than race and sectarianism (as they share the same race and religious sect "Hanifi'te" with Tajiks/Parsiwans), views Iran as the primary supporter of the Persian language in Afghanistan. Pashtuns believe that if Iran had not imported Persian books into Afghanistan, the Pashtu language would have had a wider prevalence in the country. Thus, the Taliban's policy towards Tehran would be to prevent Iran from supporting Persianate literature and to attract Tehran to support and enrich cultural programs in the Pashtu language.

The Taliban's sectarian and politicized Deobandi-based religious interpretations see Iran as a "*Rafidi*"⁴ state, with anti-Shi'ism being an institutionalized memory among those with a radicalized understanding of Islam. The Taliban have attacked Shia gatherings and beheaded Shia minorities in different central towns and provinces. The so-called Islamic State of Khurasan, ISK, shares the same mentality against Shi'as. Therefore, the Taliban sees Iran as a threat to Islam since they consider it a Shia state. Since they took power, the Taliban has expressed their views on the Sunni minority's rights several times.

The same applies to the relationship between the Taliban and Pakistan. The Taliban's honeymoon with Pakistan will not last long either. The Taliban's "Pashtun nationalism" will soon be pitted against Pakistan, tied to the Pashtuns behind the Durand Line. Pakistan had supported the Taliban as a strategic asset to debunk Pashtun nationalists in Kabul who did not raise or support secessionism in Pakistan led by the Baluchi and Pashtuns of Pakistan. However, the tribal memory of Pakistan's phobia will turn the Taliban against Islamabad soon. This scenario was repeated during the rule of the Mujahideen in Afghanistan, who had the full support of Islamabad in fighting against the Moscow-backed government in Kabul. Yet, upon arriving in Kabul, they attacked Pakistan's interventionism and expansionist policies.

⁴ Radida or Rafidi refers to Shi'i Muslims who reject (rafid) the caliphates of the first two successors of the Islamic prophet Muhammad: Abū Bakr and 'Umar (Encyclopedia Britannica, 20 July 1998), who are the Rightly Guided Caliphs for Sunnis.

The Taliban believe that there is no actual Islamic state in Pakistan; therefore, Jihad should be extended and continued in Pakistan. Several commentaries by second-rank leadership of the Taliban have criticized Pakistan's un-Islamic government. This institutionalized mentality is shared among all the Islamists in the Af-Pak region. The symbiotic relationship between the Afghan Taliban and Pakistani Taliban over a decade has influenced the views of the Afghan Taliban. While the top leadership may have a diplomatic and conservative position against Pakistan, the ground realities show the opposite. If the *Pakistani Tahreki Taliban* (PTT) initiates military operations against the Pakistani regime, thousands of Afghan Taliban will join them. Many Afghan Taliban fighters have made such claims through videos and interviews.⁵

The relations between the Taliban and Central Asia are more predictable, as states like Tajikistan, Uzbekistan, and Turkmenistan are politically driven and exhibit linguistic nationalism and tribalism. They share common ethnic and linguistic relations with Afghanistan but reject the politicized Deobandi interpretation of Islam espoused by the Taliban, favoring instead a Balkh-Bukharan theological interpretation prevalent throughout Central Asia. Therefore, the Taliban views these three countries, and the rest of Central Asia, as a threat to their survival.

Although Moscow's accommodating policy towards the Taliban, accepting them as a ground reality and anti-US asset, resulted in conservative policies towards the Taliban in Central Asia, the Taliban would not see Central Asian countries as allies. Despite the three pillars of Taliban objectives, thousands of Tajiks, Uzbeks, and other Central Asian citizens have fought alongside the Taliban against NATO allies and Afghanistan's National Defense and Security Forces (ANDSF). They have been stationed in Kabul, awaiting an opportunity to conduct their operations in Central Asia by crossing the Amu River. Previously, we have seen Tajik terrorist groups enter remote areas of Tajikistan through Badakhshan and behead some of Tajikistan's security forces.

The Taliban are also wary of these intolerant and radical Central Asian fighters. If the Taliban try to deport or banish them from Kabul and other major cities under their control, these fighters may join ISK and turn against the Taliban. The Taliban leadership understands that their Central Asian allies have carried out many attacks against international forces and the ANDSF. Therefore, there is a symbiotic relationship between the Taliban and the Central Asian radical groups, which could damage the Taliban's efforts to maintain cordial relations with Dushanbe, Tashkent, and Ashgabat.

⁵ Makhdoom Shahab-ud-Din, "Video | Taliban Chief Announcement After Cutting Fence Wire Erected by Pak Army at Durand line Border," *Youtube.com*, 2021, www.youtube.com/watch?v=Y9mz8IliiOg.

The Taliban do not consider the Kingdom of Saudi Arabia a natural ally. According to the Taliban's ideology, Saudi Arabia is an ally of the US and has a corrupt leadership that supports the suppression of Muslims worldwide.⁶ This view has been prevalent among Taliban fighters, particularly under the supervision of Afghan-Arab jihadists who joined the jihad in Afghanistan in the 1980s. One of these ideologues was Abdullah Azam, a top Afghan-Arab leader. Thousands of Arab fugitives later joined the Taliban from 1994 to 2001 and then from 2003 to 2021 to fight NATO-allied forces. These fighters have further solidified the Taliban's anti-Saudi stance through writings, preaching, and orations.

The Pakistani and Saudi finances and military did initially support the formation of the Taliban and their earlier victories. However, soon after the Taliban seized power in Kabul in 1996 and kept their hospitality towards Osama bin Laden, Saudi Arabia turned against the Taliban. This contributed to the Taliban's loss of power at the turn of the century. Therefore, the Taliban still do not have cordial relations with Riyadh.⁷

India, China, and Russia also oppose the third pillar of the Taliban ideology, its radical interpretation of Islam (not including the linguistic and Pashtunwali aspects). Many Taliban leaders and commanders have formed alliances with Indian Kashmiri fighters, Chinese Uyghur separatists, and Russian jihadists in the Caucasus. They believe that in all three countries, minority Muslims are oppressed and support the independence movements of Kashmir, Xinjiang, and the Caucasus nations, which they have idealized since the Afghan Jihad (1979-1992). During their previous rule (1996-2001), the Taliban even allowed the Chechen embassy to operate in Kabul's Wazir Akbar Khan area.⁸ Many Taliban fighters have also joined the insurgency in Kashmir and fought against Indian security forces.⁹ The Taliban has close ties with the East Turkistan Islamic Movement (ETIM) in the bordering areas between Pakistan and Afghanistan, and there are reports that Al Qaeda was training both Taliban and ETIM fighters in the same camps. Therefore, it is unlikely that their allies who have fought alongside them or joined their jihad will not respect or sympathize with the Taliban regime after it seizes power.

⁶ Nawaf E. Obaid, "The Power of Saudi Arabia's Islamic Leaders," *Middle East Quarterly* (September 1999): 51-58, <https://www.meforum.org/482/the-power-of-saudi-arabias-islamic-leaders>.

⁷ Mirwais Balkhi, *Saudi Arabia's Foreign Policy Towards Afghanistan; 1991-2014* (Kabul, Afghanistan: Afghanistan Institute of Higher Education, University of Afghanistan, 2014), 113. – in Persian/Farsi.

⁸ Thomas D. Grant, "Current Development: Afghanistan Recognizes Chechnya," *American University International Law Review* 15, no. 4 (2000): 869-894, 869, <https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1276&context=auilr>.

⁹ Ijaz Khalid, "Sino-Russian Stance on Kashmir Issue," *Global Strategic and Security Studies Review* 5, no. 1 (Winter 2020): 47-56, https://gsssrjournal.com/papers/GVFULSI_XTQ.pdf.

The linguistic pillar does not inform the Taliban's policy towards the West; instead, their respective policies are defined by Pashtunwali and a radical interpretation of Islam. According to the Taliban's ideology, the US, NATO, and the European Union are viewed as imperialistic and colonial powers that invaded Afghanistan with the aim of westernizing the country. Although they may change their diplomatic stance towards the West to seek recognition and humanitarian support for the Afghan people under their control, ideologically, the Taliban still reject the West and adhere to a jihadi approach. The memory of their worst defeat by the US-led forces in 2001, in which they lost their power and thousands of fighters were killed or imprisoned, remains bitter in their minds. The Taliban will continue to fight against Western domination by providing shelter and training to global terrorists and engaging in drug smuggling. They do not believe that the Emirate is capable of fighting a conventional war against NATO forces and would prefer a non-conventional approach using terrorist tactics and drugs.

Regional Approaches towards the Taliban

This section of the article examines how involved countries such as Pakistan, Iran, neighboring Central Asian states, India, China, and, Western nations perceive the Taliban and their interests in the region.

Pakistan

Pakistan holds a unique position among all other countries involved in the Afghanistan dispute. The Pakistani armed forces have developed military approaches and strategies, and the leadership in Islamabad has persistently attempted to stabilize and extend the Taliban's military power, and legitimize them after the fall of Mazar-i-Sharif in 1997. These are considered prominent examples of Pakistan's active policy and diplomatic efforts towards the developments in Afghanistan. Pakistan's diplomacy has been successful in Afghanistan due to various internal and external reasons. Islamabad's foreign policy includes attempts to influence Afghanistan and achieve some of its national goals.¹⁰

Pakistan played a crucial role in the creation and support of the Taliban, using them as a political, economic, and military tool. With the assistance of intelligence agencies from the US and UK, as well as financial support from Saudi Arabia, Pakistan was able to improve its trade route with Central Asia and address the issue of Pashtunistan by leveraging Afghanistan's strategic location. Pakistan has consistently opposed a strong government in Kabul that could threaten its

¹⁰ Sayyid Abdul Qayoom Sajjadi, "Taliban, Iran and Pakistan: A Study of Foreign Policy of Iran, Pakistan and Saudi Arabia towards Taliban: Since Mazar-e-Sharif Fall Apart," *Uloomi Siyasi Journal*, no. 2 (2009), 249, accessed December 20, 2021, <https://hawzah.net/fa/Article/View/84390/>.

interests or revive old conflicts. As such, Pakistan prefers establishing and maintaining governments like the Taliban in Afghanistan, which it can easily manipulate to achieve various strategic goals.¹¹

Pakistan's interests in Afghanistan can be classified into three main layers:

1. **Geopolitical Goals:** Pakistan seeks to establish a weak and compliant government in Afghanistan, disregarding the Durand Line dispute, and weakening Afghanistan's national power and capability. This is aimed at reducing the risk of Afghanistan posing any threat to Pakistan's interests or reviving old conflicts.
2. **Geo-economic Goals:** Pakistan aims to gain direct access to the Central Asia region and clear the vital transit route between Pakistan and the Central Asian markets. It also seeks to access the oil and gas resources of the Central Asian countries and turn Afghanistan into a market for consumer goods.¹² The establishment of the Taliban in Afghanistan is seen as a means to achieve these goals.
3. **Geostrategic Goals:** Pakistan's strategic competition with India defines the balance of power in South Asia. As the intermediary neighbor between Afghanistan and India, Pakistan seeks to maintain a superior status. To achieve this, it aims to prevent India from influencing Afghanistan and prevent the formation of regional alliances between Iran, Russia, and India, or India and the United States, in relation to Afghanistan.¹³

The Taliban's control of Afghanistan serves Pakistan's interests by providing a friendly government that supports its goals of geopolitical, geo-economic, and geostrategic influence in the region. If the Taliban were to be removed from power, that would limit Pakistan's ability to achieve these goals and could potentially strengthen the position of its rivals in the region.¹⁴

Iran

The Islamic Republic of Iran is a significant player in the Afghanistan conflict. The Taliban's rise to power in Afghanistan was unexpected and concerning for Iran. Iran views the Taliban as a dangerous group that receives support from regional countries and global powers. Iran believes that the Taliban seeks to undermine

¹¹ Aqajari et al., "The Role of Regional Players in Post-Taliban State Building of Afghanistan," *Pazhohishnamai Ravabit Bainulmilal*, no. 30 (2015): 57-104, 67.

¹² Nawzar Shafiee, "Power Politics in Afghanistan: Objectives and Behavioral Patterns," *Mujala'i Siyasati Difah'i*, no. 20 (2002): 29-58, 35.

¹³ Umul Banin Tawhidi, "Afghanistan Issues: the US and Others," *Mah'awinat Pazhohishhai Siyasati Khariji*, no. 301 (2009): 64-87, 11.

¹⁴ Shafiee, "Power Politics in Afghanistan," 66.

the true teachings of Islam and limit Iran's regional policies through their extreme interpretation of religion and oppressive tactics.¹⁵ While Tehran may view the Taliban as an anti-US ally, it has not forgotten how the Taliban previously ignited a war with Iran by killing Iranian diplomats and threatening its security. The US-led invasion of Afghanistan, which resulted in the overthrow of the Taliban, was initially seen by some as beneficial to Iran as it removed an ideological rival and an explicit security threat. This shared objective between Iran and the United States suggests a potential for cooperation and natural unity.¹⁶

Tehran has adopted a "wait and see" approach towards the Taliban's takeover of power in Afghanistan but remains skeptical of its former ally. The sudden and dramatic takeover of Kabul by the Taliban has left Tehran unsure of how to proceed. Despite its longstanding opposition to the Kabul regime, Iran has been cautious about engaging with the Taliban since the minor clash between Taliban fighters and Iranian border security guards in Nimruz province in December 2021. Iranian strategic communities are grappling with the unpredictability of the situation, particularly regarding the US empowering the Taliban and the fate of the military equipment seized by the Taliban from the US and Afghan National Defense and Security Forces (ANDSF). Tehran's traditional saying, "a wise enemy is better than an ignorant friend," has left it feeling defensive and apprehensive about the Taliban's intentions.

Saudi Arabia

Despite being one of the most significant economic resources of Sunni jihadist groups and parties within the framework of its ideological strategic policies since the Afghan jihad from 1994-1996, Saudi Arabia has not played a big role in the Afghanistan conflict. The Saudis' supportive policies towards the Taliban peaked in 1996 when Saudi Arabia, as the primary financial source of this group, played a substantial role in helping the Taliban eliminate all other parties and groups from the military arena in Afghanistan. Since Prince Turki Al Faisal, director of Saudi Arabia General Intelligence Directorate, visited Pakistan in July 1996, Saudi Arabia has become the principal financial supporter of the Taliban.¹⁷ However, the Kingdom has security concerns with the anti-Saudi Islamists who have taken shelter under the Taliban's safe haven.

Furthermore, some circles and groups within Saudi Arabian religious circles have had an active physical presence at the battlefield, supporting the Taliban against the ANDSF/NATO alliance, although some have mainly held memberships in other radical jihadist parties like ISK. After the US troop withdrawal and the collapse of the Afghan government, these forces now live safely in Kabul

¹⁵ Ibrahim Ahmadi and Jawad Etahat, "A Geopolitical Analyses of Pakistan Relations with Others: Conflicts and Threads," *Tahqiqat Bainulmilali Journal*, no. 24 (2015): 1-24, 17.

¹⁶ Dehqani Firuzabadi and Sayyid Jalal, "Iran's Foreign Policy Towards Afghanistan's Crisis," *Pazhohishi Hoqq wa Siyasat*, no. 20 (2006): 7-22, 11.

¹⁷ Sajjadi, "Taliban, Iran and Pakistan: A Study of Foreign Policy."

without any engagement. Consequently, they may focus on their primary objective of conducting terror attacks on Saudi Arabia or any other target worldwide. Saudi Arabia's conservative policy towards the Taliban and Afghanistan will likely become more active. It is worth noting that the embassy of Saudi Arabia in Kabul was not among the four embassies that remained open and running consulate operations on August 15 when the Taliban entered Kabul.¹⁸ Although some Pakistanis may try to tie relations between Riyadh and the Taliban, Saudi Arabia does not trust the Taliban much.¹⁹

India

With the assistance of Pakistan's Inter-Services Intelligence in both periods (1994-2001 and 2003-2021), the Taliban's rise to power in Afghanistan has been alarming to India. It has resulted in undesirable outcomes for the country. After the Taliban seized control of Kabul on August 15, the Embassy of India in Kabul closed, and political relations with the Taliban government were cut off because the Indian government did not recognize the Taliban's legitimacy. Furthermore, India regards the Taliban's ideology as a threat to its security, as the spread of their ideas in the Jammu and Kashmir region poses a danger to India's safety and unity.²⁰ The Taliban's ascension to power with the assistance of Pakistan, India's longtime rival, has limited any potential benefits for India. Access to Central Asian energy resources is of critical importance to India, and establishing military bases in some Central Asian countries is one of India's strategic objectives.²¹

India was the only country among those present in Afghanistan that did not support the Taliban, but this strategy is no longer relevant. The Bharatiya Janata Party's pragmatic foreign policy is focused on limiting Pakistan's influence, and supporting Afghan/Pashtun nationalism has been a top priority. India quickly recognized the fraudulent government of Mohammad Ashraf Ghani, and the Indian strategic community is advising policymakers to explore opportunities to establish ties with the Taliban by leveraging Pashtun anti-Pakistan sentiment. India seeks to attract the Taliban's attention toward Delhi and create a triangle of Taliban-Pashtun Nationalists in Khyber Pakhtunkhwa and New Delhi to exert pressure and possibly undermine Pakistan.

¹⁸ The four embassies which remained open on the days of uncertainties and insecurities were Pakistan, Iran, China, and Russia. The rest had left Afghanistan weeks before or on the day of the collapse. Among the earliest evacuations was that of the Saudi Arabia's embassy.

¹⁹ Suhasini Haidar, "Taliban Have Responsibility to Exercise Good Governance, To Be Inclusive: Saudi Foreign Minister," *The Hindu*, September 19, 2021, <https://www.thehindu.com/news/national/saudi-foreign-minister-faisal-bin-farhan-al-saud-interview-taliban-have-responsibility-to-exercise-good-governance-to-be-inclusive/article36556729.ece>.

²⁰ Aqajari et al., "The Role of Regional Players in Post-Taliban State Building," 74.

²¹ Nawzar Shafiee et al., "India's Approach towards Afghanistan after September 11," *Geopolitical Journal*, no. 2 (2012): 91-126.

Trans-Regional Approaches towards the Taliban

The US

The September 11, 2001, attack on the Twin Towers by Al-Qaeda led to the US attack on Afghanistan. The attack occurred when the US was at the height of its power and could dominate the new world order following the Soviet Union's dissolution. Consequently, since 9/11, the United States has identified new threats and enemies, and counter-terrorism has become a geopolitical priority in US foreign policy. A geopolitical code is a set of political-geographic assumptions that guide a country's foreign policy towards locations beyond its borders. Countries aim to influence other countries' geopolitical codes to achieve their goals and interests. Fighting terrorism became a priority, and Afghanistan, which provided a safe haven for Al-Qaeda, became strategically significant in terms of geography, economy, and geopolitics.

The policy of the United States towards Afghanistan underwent a significant shift in the early 2020s. Many geopolitical rivals seeking to use Afghanistan to their advantage, including China, Russia, and Iran, supported the Taliban and opposed the US presence in Afghanistan. There were even reports of direct Chinese attacks against US military forces.²² After twenty years of war, the US became exhausted and shifted to a policy of deterrence and diplomatic alliances to guard against potential threats from Afghanistan. However, the US continues to closely monitor the Taliban and has indicated that it is willing to engage in unconventional warfare if necessary.

Russia

The countries of the former Soviet Union are considered influential actors in Afghanistan's changing circumstances. Afghanistan's situation has a significant impact on Tajikistan, while Turkmenistan is not practically capable of exerting influence on Afghanistan. Uzbekistan prioritizes its national security, and Afghanistan's stability is crucial in that regard. Russia, as the most important actor of the Commonwealth of Independent States, aims to prevent Islamism from becoming the common political agenda of the Central Asia region. From Russia's perspective, Afghanistan is a source of violence and illegal trade, including drugs and weapons, and a major exporter of extremist Islamism. This view is reinforced by the historical experience of Islamist groups such as the Islamic Movement of Uzbekistan, an extremist Islamic group trained by the Taliban in the 1990s and still supported by them. During the civil war, the Islamic Renaissance Party of Tajikistan established military bases and financial resources in the northwestern areas of Afghanistan.

²² اظهار بی‌اطلاعی چین از اخراج شهروندان اش از افغانستان به اتهام جاسوسی [China's statement of ignorance about the expulsion of its citizens from Afghanistan on charges of espionage], *Deutsche Welle*, January 8, 2021. – in Farsi.

Moscow maintained ties with the Taliban until the United States withdrew from Afghanistan. At the same time, Russia has expressed security concerns about international terrorist groups operating alongside the Taliban. If future clashes erupt due to the Taliban's lack of effective control over Afghanistan's northeastern borders, these relations could quickly deteriorate and destabilize the region. Furthermore, Russia is worried about the Taliban's vulnerability to extremist groups, as it considers these groups to be the most significant threat to stability in Central Asia. Additionally, the movement of people between Central Asian countries and Afghanistan has facilitated the development of extremist Islamic ideologies in religious circles.²³

European Union

The European Union has been involved in the Afghanistan conflict since terrorism and organized crime were identified as severe threats to Europe. Afghanistan is a critical case for the EU's fight against terrorism, and the Union seeks to expand its influence as a global actor by promoting its approach to conflict management and peace establishment. However, EU member states have differing views on their role in Afghanistan. Some states, not primarily concerned about terrorism, worry that their defeat in Afghanistan would damage the credibility of NATO and the West. Other countries are present in Afghanistan due to their deep strategic relations with the US. At the same time, some believe that their security (excluding the UK) depends on Afghanistan's situation, leading to their commitment to the US alliance. Although the European governments do not play a militarily dominant role in Afghanistan, they offer international aid within the Union's framework or through bilateral agreements to ensure Afghanistan's security and stability.²⁴

What Should Be Done in the Future?

In the author's view, both regional and faraway countries involved in the Afghan conflict should adopt a "wait and watch" approach toward the Taliban. A dual strategy is required, with a fundamental political approach aimed at finding a long-term solution to Afghanistan's conflict while providing immediate humanitarian aid to the people. Here are some suggestions:

- The Taliban's current efforts are aimed at gaining recognition, and all states should be cautious in this regard. Supporting the Taliban regime, in the long run, will not benefit anyone and may result in losing strategic friends in Afghanistan, particularly the ordinary people. On the other

²³ Mohammad Darkhor, "Regional and Trans-Regional Strategic Approach towards the US Withdrawal from Afghanistan," *Rahnama Siyasatguzari Journal*, no. 2 (2012): 53-67, 62.

²⁴ Yaser Nooralivand and Ali Khalilipour Roknabadi, "Multilateralism and Trans-Atlantic Relationship in Afghanistan," *Strategic Studies Quarterly* 14, no. 51 (June 2011): 175-200, 187, <https://doi.org/20.1001.1.17350727.1390.14.51.7.9>.

hand, the Taliban is keeping an eye on US support, and yesterday's strategic enemies may seek to become tomorrow's friends.

- The international community can provide humanitarian aid and support to Afghanistan. Countries that have experience with the Taliban, such as providing monetary aid in the 1990s or experience with soft measures, can share their expertise. The co-education model and approaches to girls' education in Pakistan, Iran, Saudi Arabia, and other regional countries are good examples to follow.
- It is crucial to continue the policy of exporting goods from neighboring countries to Afghanistan, as this is vital to the people's welfare and may help reduce cross-border tensions. On the other hand, closing borders and terminating trade will harm the people.

Conclusion

The emergence and coming to power of the Taliban in Afghanistan have led to different strategies adopted by regional and trans-regional actors. Pakistan and Saudi Arabia have supported and financed the Taliban, viewing it as a means to further their regional interests. However, Iran, India, and Central Asian countries have expressed concerns and perceived the Taliban as a threat to their regional interests. Trans-regional approaches to the Taliban's rise to power also differ significantly. At the start, the United States did not consider the group a threat to its interests. However, the September 11 attacks, Osama bin Laden's sheltering in Afghanistan, and the group's violent nature caused the United States to change its position and seek to defeat and dismantle the terrorist organization. The European Union's policies towards the Taliban, based on NATO's invocation of Article 5, are also noteworthy. In contrast, Russia views Afghanistan as a source of violence, drugs, and weapons and an exporter of extremist Islamism that threatens its own and the interests of neighboring countries in Central Asia. Therefore, Russia does not view the Taliban positively as a trans-regional actor in Afghanistan.

Generally speaking, there are divergent views on the Taliban at both regional and trans-regional levels. While some have expressed optimism about the group's emergence, others have taken a more pessimistic view. The Taliban's entry into the political arena of Afghanistan has resulted in the formation of multidimensional policies and varying perspectives in the international arena.

Disclaimer

The views expressed are solely those of the author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

About the Author

Mirwais Balkhi, Ph.D., is a Visiting Scholar of International Relations and Middle Eastern Studies at Georgetown University Qatar. He has an extensive background in government and academia, having served as the Minister of Education of the Islamic Republic of Afghanistan from 2018 to 2020 and as Afghanistan's Deputy Ambassador to India. Dr. Balkhi received his Ph.D. degree in international relations with a specialization in West Asia from Jawaharlal Nehru University in New Delhi, India. He is a prolific writer, having published numerous academic articles in both English and Persian. Before joining Georgetown University in Qatar, Dr. Balkhi was a lecturer at the Law and Political Science Faculty of the American University of Afghanistan (AUAF) and at the International Relations Faculty of Afghanistan's Institute of Higher Education (UofA).

E-mail: mirwaisbalkhi@yahoo.com

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 PfPCpublications2@marshallcenter.org or uploaded to the journal website via <https://connections-qj.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. Additionally, authors should provide a manuscript abstract and keywords.

Preferred themes for future journal editions include:

- Post Conflict Management
- Countering Hybrid Warfare
- Bolstering the North Atlantic Alliance
- Competition for Resources and Its Impact on Security
- Non-State Actors in Cyber Space
- Emerging and Disruptive Technologies
- Digital Transformation and Security
- Defense Institution Building
- Reducing Corruption and Building Integrity
- Enhancing Defense Education

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.

For all information regarding CONNECTIONS, please contact:

Partnership for Peace – Consortium
Managing Editor – LTC Ed Clark
Gernackerstrasse 2
82467 Garmisch-Partenkirchen, Germany
Phone: +49 8821 750 2259
E-Mail: PfPCpublications2@marshallcenter.org

ISSN 1812-1098
e-ISSN 1812-2973

