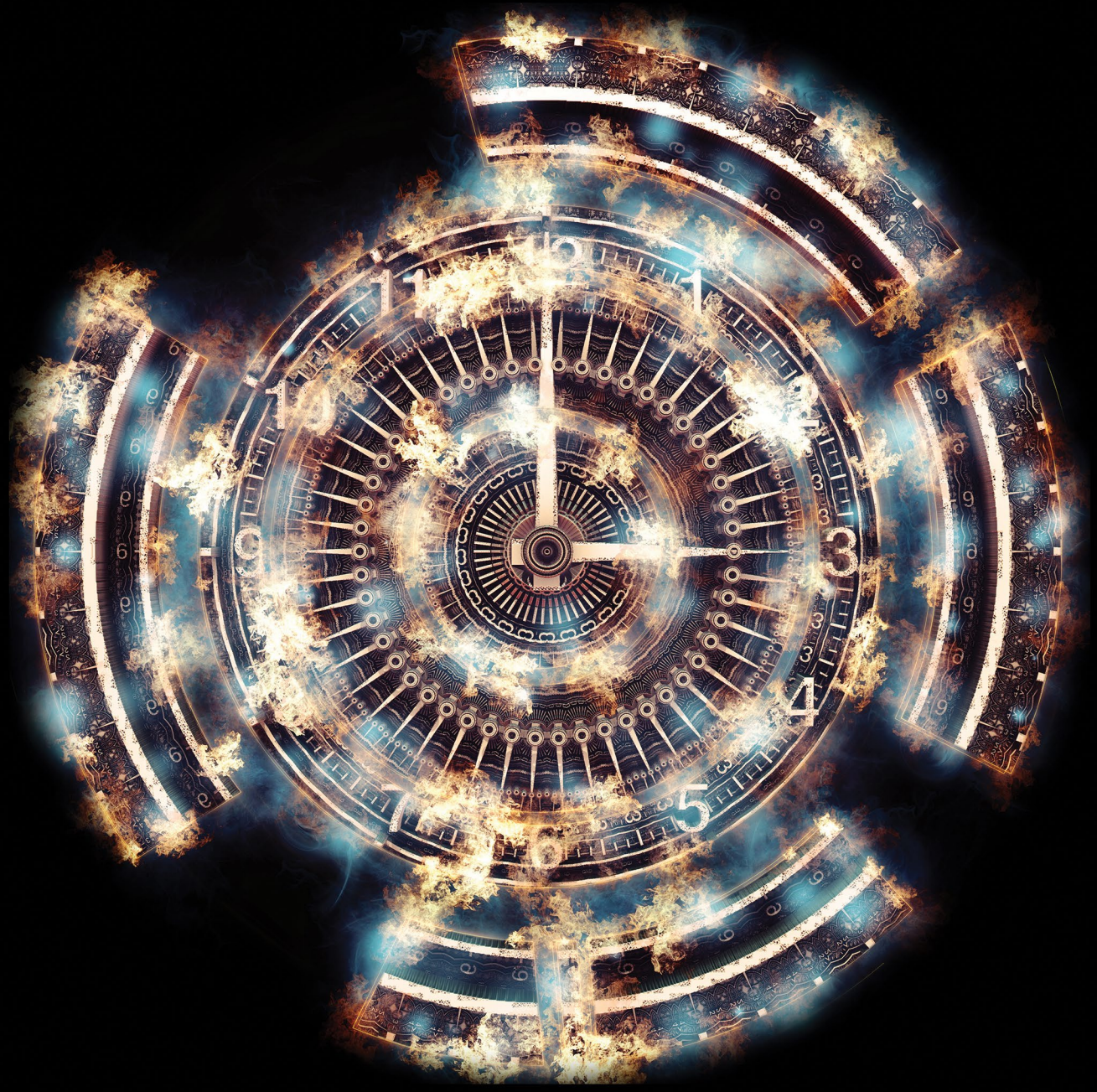
Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY



# ALTERNATE CYBERSECURITY FUTURES

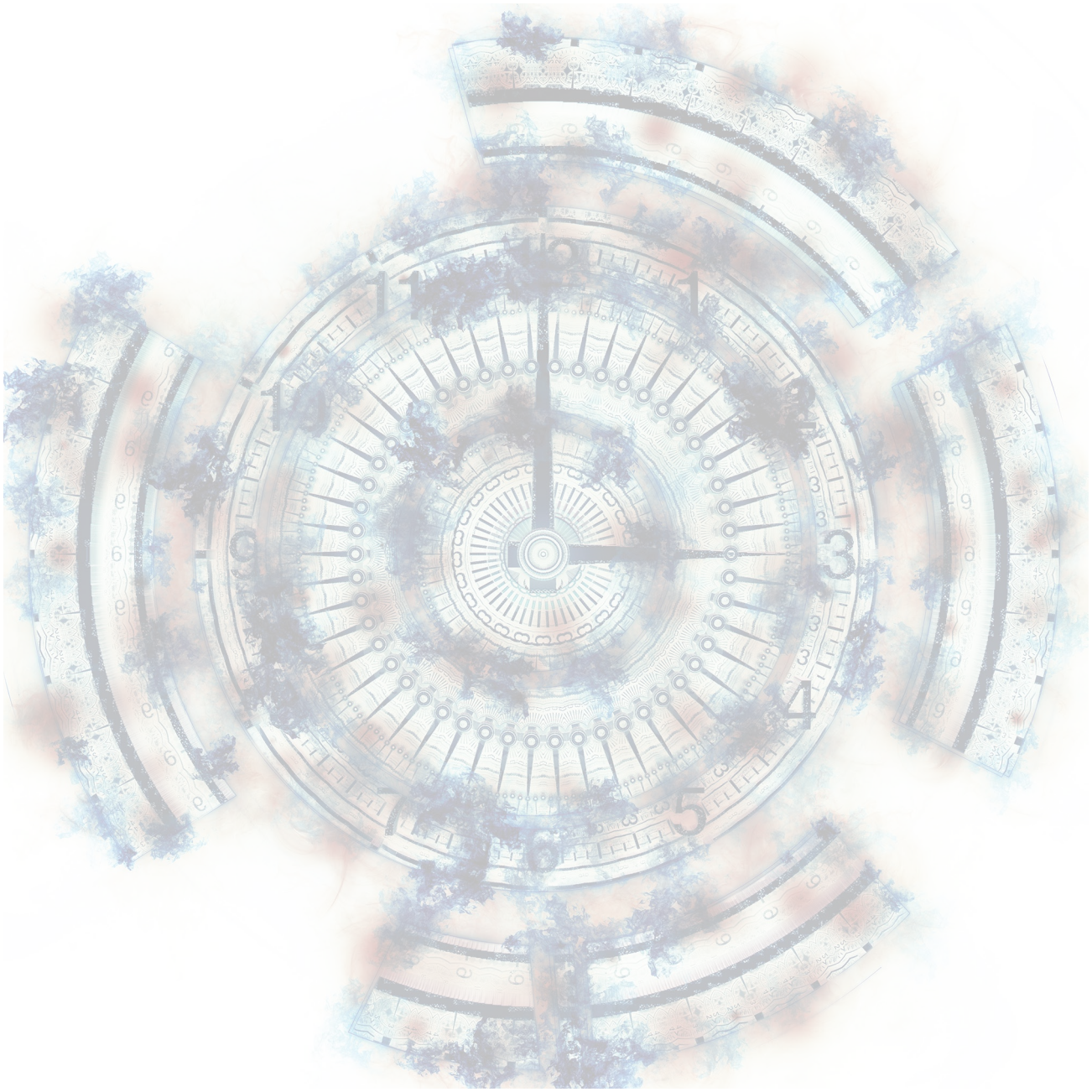
John Watts · Ben Jensen · JD Work · Chris Whyte · Nina Kollars

# MISSIONS

**The Scowcroft Center for Strategy and Security** works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.

The focus of the **Cyber Statecraft Initiative** is to:
1) Examine the nexus of geopolitics and national security with cyberspace;
2) Continue to build out the new field of cyber safety in the Internet of Things; and
3) To help build the next generation of cybersecurity and cyberspace policy professionals.
Throughout all of its work, the Initiative focuses relentlessly on providing practical, innovative, and relevant solutions to the challenges in cyberspace. The Initiative brings together a diverse network of respected experts, bridging the gap between the technical and policy communities.

The mission of the Atlantic Council's **Emergent Futures Lab** is to explore emergent issues that may seem fringe, implausible, or unpredictable today, but which have the possibility to cause significant disruption in the future. Emergent challenges can be detected but not yet fully discerned. They do not necessarily follow predictable trendlines, and therefore cannot be extrapolated solely from an analysis of plausible or likely current or near-term events. But they are likely to be disproportionately disruptive and impactful. The Emergent Futures Lab seeks to prepare for these eventualities by using a range of creative and non-traditional methodologies that explore the 'what-ifs'. While remaining anchored by practical real-world constraints, these methodologies open the aperture of possible future outcomes.



# ALTERNATE CYBERSECURITY FUTURES

John Watts · Ben Jensen · JD Work · Chris Whyte · Nina Kollars

ISBN-13: 978-1-61977-595-4



September 2019

# CONTENTS

# FOREWORD

The forward march of advanced technologies, especially information technologies, and their integration into all aspects of society are creating tremendous opportunities—and an associated set of vulnerabilities. Both 5G networks and the Internet of Things (IoT) are going to connect us further in ways only limited by our imaginations. While this growth has been forecasted over the past few decades, few saw the scope and breadth of the implications, both positive and negative, on our society. The Department of Defense has recognized that hardware, software, and data now connect in ways that have created a cyber domain, much like the land, sea, air, and space domains. The implications have manifested themselves in the relentless competition underway between those that defend and those that attack on a continuous basis. This evolution in our thinking on the cyber problem demands strategic analysis. Numerous reports have been generated over the past several years, with thousands of recommendations. Yet, the problem only continues to grow.

One of the primary reasons for this growing problem is a strategic-forecasting problem. Some say the future is unknowable because technology is moving too fast. Some say the problem is in our structures, laws, and policy—i.e., the use of nineteenth- and twentieth-century rule sets for a twenty-first-century world. Some blame the private sector for not building in security from the start. Others are worried about the militarization of cyberspace. Nation-states with cyber capabilities have diverse views on the concepts, technologies, and norms. Criminal activity moved to the money. The bottom line: there is a plethora of reasons why we are where we are, but little broad consensus on the problems or the way ahead. As a result, many actions are primarily reactive in nature.

It is time to change our thinking, and to create a strategic framework for future action that can be much more proactive. One technique to do this is to project our thinking forward into the future by creating different future scenarios. Could we have predicted the impact of the explosion in information technologies, in terms of both opportunities *and* vulnerabilities? Could we have predicted the weaponization of information over time, as demonstrated by Russia's actions in Estonia, Georgia, Ukraine, and eventually, the United States? It is widely known that China has been stealing intellectual property for years. It is also widely known that both Iran and North Korea have conducted destructive cyberattacks against Saudi Aramco and Sony Pictures, respectively. The conceptualizing of future scenarios is an effective tool to describe and predict possible future outcomes and, more importantly, to work backward from the future to describe what might be accomplished in the present to position ourselves to modify, alter, or change the future within a competitive environment.

Forecasting is extremely difficult; some say it is impossible. That said, crafting a set of potential alternate futures, with a series of waypoints or decision points that validates or invalidates a given path or assumptions, *is* possible now. This approach drives action forward, and the competitive environment forces the normal action-reaction-counteraction competitive framework for action. Some change may be gradual, and some may be dramatic. What is most important is the ability to modify, adapt, or even pivot at speed across concepts, technologies, structures, and frameworks on a continuous basis, which creates a competitive advantage over time. This report starts that effort.

***Lieutenant General Edward C. Cardon (US Army, Retired)***

# INTRODUCTION

In any given period of history, the ways in which people connect evolve based on available technologies and social norms. As people connect, power flows. From sea lines of communication and trade winds to railroads and 5G cellular networks, connectivity creates channels of influence and drives competition. Understanding how these connections evolve is critical to defining the future operational environment and the resulting character of strategic competition. As revisionist states leverage disruptive technologies to undermine US interests across the world at a level beneath the threshold of armed conflict, this digital gray zone sees near-constant espionage, sabotage, and influence operations.[1] New classes of actors emerge, beyond traditional states and their proxies, to include business and social networks willing to conduct unilateral, offensive actions. Unlike military force, governments have never had a monopoly on cyber capabilities, and their grip on this domain could slip further in years to come.

In this new epoch, key technologies and social understandings become critical capabilities on the digital battlefield. Technological developments converge and create new risk vectors. Artificial-intelligence and machine-learning (AI/ML) capabilities combined with scaled data sets could offer ways to exponentially amplify information-warfare campaigns. This prospect threatens destabilizing incentives for an AI arms race, while enabling social engineering at scale and shortening the window for defenders to adapt. Our virtual lives continue to expand, destabilizing status-quo political arrangements and creating new opportunities for social media intelligence gathering and data poisoning as a form of social defense. The battlefield is as amorphous as at any point since the birth of the Westphalian state.

This emerging character of strategic competition developed rapidly, iteratively, and organically, as growing connectivity changed how groups compete for power and influence. As such, it is easy to miss the magnitude of this evolution and the resulting implications. If the national security community continues to focus on immediate threats and managing current emergencies, it will never escape a cycle of crises, nor manage to impose a strategy to shape tomorrow's environment. Taking a step back is important to appreciate both the state of cyber competition today and where the trends might lead tomorrow. To create new concepts of response, we need to first appreciate the reality we live in and the various ways in which it may change, so that we can be frank about how we should respond in the future.

Visualizing and describing the evolution of cyber capabilities and strategic competition require envisioning multiple futures. The more complex a scenario becomes, or the longer the time horizon, the more important it is to think across a range of trends to describe alternative futures. These depictions help strategists identify critical vulnerabilities and opportunities for pursuing national interests. They also point to an optimal combination of ends, ways, means, and risk to achieve those objectives. At the Scowcroft Center for Strategy and Security, strategic foresight is a core part of our mission, as it is the foundation for developing sustainable, nonpartisan strategies. In this, good strategy starts with thinking broadly about alternative futures.

This report was developed from just such an ideation activity. The Emergent Futures Lab and Cyber Statecraft Initiative convened cybersecurity and national security experts to consider how prominent trends and wild-card factors could shape the future, and what implications this might have for the United States. From this discussion, the authors have distilled three scenarios, each centered on a single theme that addresses a different facet of future cyberspace with two trends and their implications. Across all three scenarios, the authors identified further alternative futures, which are summarized in the conclusion.

Conventional processes to generate understanding are beset on all sides as institutions risk preparing to fight the last war. Change on the scale taking place is difficult to conceptualize; how individuals determine what is known shifts with technological and commercial change, and they must react to ever more clever manipulation and abuse. These scenarios are not intended as a summary of a single ideation event. Rather, they are meant to be the next step in a critical discourse that can only achieve its aim if continued, challenged, iterated, and expanded upon. This report is not the last word, nor the first salvo, but a means to an end. Contemplate these futures and consider how long it might take to run from today to one of these tomorrows. The time we have may not be enough.

1 Benjamin Jensen, "The Cyber Character of Political Warfare" *Brown Journal of World Affairs 24, 1 (2017), http://bjwa.brown.edu/24-1/benjamin-jensen-the-cyber-character-of-political-warfare; Brandon Valeriano, Benjamin Jensen, and Ryan Maness, Cyber Strategy: The Evolving Character of Power and Coercion (New York: Oxford University Press, 2018).*

# SCENARIO 1—A State of Risk and Friction:

## *Luctare adversus omnium potestātēs'* (The struggle of all, against all powers)

J.D. Work

### SETTING

Great-power competition has reemerged as the prevailing force shaping national security strategy, defense expenditures, and, as a result, cyber operations. Even as the democratization of technologies results in the proliferation of threat actors—both in their quantity and diversity—the capabilities of nation-states advance apace, meaning they will remain the pinnacle and key driver of the nature of cyber conflict in the near future. This has significant strategic consequences. Since World War II, the mutually assured destruction (MAD) framework has ensured conventional security stability between world powers. However, it will continue to be undermined by expanded gray-zone operations, incentivizing greater antagonism, and increasing the risk of strategic miscalculation.

### KEY TRENDS

Constant Contact Wears Thin: The credibility of offensive cyber capabilities for deterrence derives from their use, more than from mere possession. This drives states to continually demonstrate cutting-edge capabilities across an ever-changing technology stack, and risks exhausting national arsenals.

Contesting New Territory, New Sovereigns, New Equities: Part of the unremitting pressure on defenders and the counter-cyber community comes from the increasing diversity of actors—some private-sector entities, as well as some neutral, or even allied, governments—all in largely unilateral pursuit of their own equities in a virtual battlespace.

### SCENARIO

During the 2020s, the cumulative impact of individual and collective adversary advances could no longer be ignored. "The largest transfer of wealth in human history," aggravated by recurring trade wars, changed patterns of global finance, and diminishing Western control of reserve currencies and international transaction backbones, pushed the United States and its allies to the breaking point.[2] Following the collapse of further pretense regarding restraint in economic espionage, after the second Rose Garden agreement, the accelerating frequency and ever-growing severity of Chinese intrusion operations clearly demonstrated that diplomacy could not endure absent competitors' real fear of the consequences.[3]

However, economic espionage was not limited to the traditional Chinese "PANDA" or "BRONZE" intrusion sets.[4] The reemergence of economic targeting by major European powers, following a series of cascading attempts to exit from the constraints of Brussels' bureaucracy and European Central Bank monetary policy—some more successful than others—drove unanticipated pressure for nonpublic information to support individual players' positions regarding taxation, customs excise, subsidy reimbursement, and a host of other disputes. These disputes were complicated by the shifting justifications for specific decisions, which arguably had less to do with the specific policy questions involving corporate governance and presence jurisdiction, and more to do with transferring wealth to shore up a continuously failing tax base.

The zoo of "ANIMAL FARM" and its neighboring "PADDOCKs" multiplied rapidly and, in so doing,

2 Josh Rogin, "NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History,'" *Foreign Policy, July 9, 2012, https://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/.*

3 For reporting on Chinese intrusion operations that may be considered in breach of the 2016 Xi-Obama Agreement, see Cristiana Brafman Kittner and Ben Read, "Red Line Redrawn? Chinese APTs Resurface," FireEye Cyber Defense Summit, October 3, 2018, https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-executive-s05-redline-redrawn.pdf; Brian Barrett, "How China's Elite Hackers Stole the World's Most Valuable Secrets," *Wired, December 20, 2018, https://www.wired.com/story/doj-indictment-chinese-hackers-apt10/.*

4 Cryptonyms reference cybersecurity industry naming conventions, in which intrusion sets attributed to specific national actors are assigned a consistent mnemonic proword.

created profound dilemmas for tech-sector firms with presences across multiple markets, and which were probably reluctant to report on malware attributed to Western government interests.[5] Non-Western and authoritarian-aligned firms faced no such concerns and gleefully outed each new detected campaign, often accompanied by unfounded and sinister allegations consistent with foreign intelligence service driven propaganda themes intended to further erode trust between the major information- and communications-technology (ICT) brands and their host nations. Targeted firms in the finance, technology, manufacturing, logistics, and legal sectors were caught in the middle. Increasingly, these companies responded through ever more elaborate ownership structures, designed to deliver compliance arbitrage under the assumption that they would be targeted for administrative fines that, in the end, would have little to do with their behavior but, rather, reflected the constantly shifting political positions of the time.

Emerging markets in Asia, the Middle East, and Latin America all saw the development of unique economic-espionage problems, as more countries sought advantage at the margins of great-power positioning to build successful business adjacencies and niche offerings, wherever agility and lack of regulation afforded options that could be accelerated through stolen proprietary information. This particularly impacted emerging biotechnology applications—including genomic editing and other human-augmentation therapies—that thrived through a demand for gray-market services catering to a medical-tourism market near frantic from the shortages and delays created by the spiraling fiscal collapse of universal medical programs that faced unsustainable promises made to gerontologic populations. Some suspected varying degrees of tacit, or even explicit, encouragement of these intrusion campaigns and their resulting product and service offerings, as they were seen as a short-term safety valve for overburdened national healthcare regimes. Nonetheless, the destruction of return on research-and-development (R&D) investment caused by such cyber-espionage-driven alternatives entering the gray market would only accelerate systemic problems within the medical industry, driving significant discontent with government and practitioners alike as morbidity and mortality outcomes continue to demonstrably worsen, and as price tags for individual treatments soar.

## MILITARY OPERATIONS IN THE INFORMATION ENVIRONMENT

The further development of cyber as a conventional military domain will almost certainly continue its inexorable trajectory, as new programs offering greater systems connectivity, interoperability, and functional expansion result in a wider attack surface and an ever-greater range of both subtle and immediate effects. Despite what may often be well-understood technology pathways, the demonstration of these effects will often result in surprise, due to innovations in the combination and employment of known capabilities in novel ways.

During a series of intermediate-range ballistic-missile (IRBM) tests by the once again military-dominated government of Myanmar, against a backdrop of heightened crisis tensions, US allies had raised increasingly serious concerns regarding overflight across their territories.[6] In several cases, missile-test failures had threatened potential debris damage and raised the difficult challenge of distinguishing a failed test event from a poorly delivered attack profile. In response, the US Indo-Pacific Command (INDOPACOM) was directed to challenge the Tatmadaw provocations and deploy an expeditionary task force to establish an early-warning and response option. A US Marine Corps (USMC) F-35B, flying from a Singapore Joint Multi-Mission Ship (JMMS), was on patrol the evening of January 11, when a Burmese Hwasong derivative launch was detected.[7]

5 ANIMAL FARM is a commonly cited intrusion set example, alleged in industry reporting to be attributed to a European intelligence service. See Marion Marschalek, "Babar: Suspected Nation State Spyware in The Spotlight," Cyphort, February 2015, http://www.infosecisland.com/blogview/24334-Babar-Suspected-Nation-State-Spyware-In-The-Spotlight-.html; Joan Calvet, "Casper Malware: After Babar and Bunny, Another Espionage Cartoon," EST, March 5, 2015, https://www.welivesecurity.com/2015/03/05/casper-malware-babar-bunny-another-espionage-cartoon/; "Animals in the APT Farm," Kaspersky Labs, March 6, 2015, https://securelist.com/animals-in-the-apt-farm/69114/; Joan Calvet, "Dino—the Latest Spying Malware from an Allegedly French Espionage Group Analyzed," ESET, June 30, 2015, https://www.welivesecurity.com/2015/06/30/dino-spying-malware-analyzed/; Pierluigi Paganini, "Animal Farm APT and the Shadow of French Intelligence," Infosec Institute, July 8, 2015, https://resources.infosecinstitute.com/animal-farm-apt-and-the-shadow-of-france-intelligence/#gref.

6 Ajey Lele, "Nuclear Myanmar: Dormancy Should Not Be Taken For Granted," *Himalayan and Central Asian Studies 18, 1/2 (2014)*, 44–52, https://www.researchgate.net/profile/Ajey_Lele/publication/289326460_AJEY_LELE/links/568b889a08ae1e63f1fd3a08/AJEY-LELE.pdf?origin=publication_list; Kelsey Davenport, "U.S. Targets Support for North Korea," Arms Control Today 48, 2 (2018), https://www.armscontrol.org/act/2018-03/news/us-targets-support-north-korea; Andray Abrahamian and Wai Moe, "Myanmar-DPRK's 'Marriage of Convenience'–Headed for Divorce?" 38 North, August 25, 2017, https://www.38north.org/2017/08/myanmar082517/; Eze Malachy Chukwuemeka, "The Limits of Sanctions as Instrument for Interest Actualisation in the International System: The Case of North Korea's Nuclear Weapons Development," Advances in Politics and Economics 1, 1 (2018), doi:10.22158/ape.v1n1p13.

7 Ridzwan Rahmat, "Singapore to Replace Endurance Class with Joint Multi Mission Ship after 2020," *Jane's 360, July 2, 2018, https://www.janes.com/article/81429/singapore-to-replace-endurance-class-with-joint-multi-mission-ship-after-2020.*

Strategic sensors, including NG-OPIR launch detection, cued the F-35 pilot to chase an incredibly fleeting moment at the edge of the aircraft's performance envelope.[8] The airframe's distributed aperture suite struggled to track and relay targeting data to the newly deployed Boost Phase Intercept system, carried as a containerized package aboard the Military Sealift Command's special mission ship attached to the task force.[9] The short engagement window forced heavy reliance upon rapid processing of sensor data at the forward edge. This was the point of vulnerability in the architecture, one that was exploited by adversary intrusion operators, who had compromised Defense Industrial Base (DIB) contractors responsible for providing maintenance support to the deployed system and introduced a modified algorithm library. Initially designed for a different threat profile under different geopolitical circumstances, the malicious code modification made no distinction between types of North Korean (DPRK) lineage missile systems and triggered a chain of rapid, minor modifications to the missile track, computed across fused sensor data. The loss of fidelity caused by compromised integrity was not apparent until the interceptor missed by the proverbial and almost literal mile, and the Burmese IRBM flew on undaunted.

## CONTESTED SOVEREIGNTY IN VIRTUAL TERRITORIES

The preeminent role played by state actors in the cyber domain did not, however, entirely exclude private players from the domain. The shifting nature of sovereignty in a post-Westphalian, or Westphalian-Plus, world has created its own collisions between the equities of ICT owners (and operators) and government interests.[10] Nowhere is this more evident than in addressing the complex challenges of lawful intercept, warranted access, and state-authorized endpoint monitoring.

The third wave of major leaks impacting IC programs—modeled on earlier, unauthorized disclosures in the ECHELON Affair, as well as the Edward Snowden defection—had a profound impact on this debate. Material purported to be stolen documents taken from the German government's Bundesnachrichtendienst (BND) intelligence service were provided by an unknown party to an ideologically aligned European Union (EU) parliamentarian. This member chose to release the material in full, under parliamentary privilege. Among other state secrets, these documents discussed POSTHARVEST, a tailored cyber-collection program implementing a "selector-less" approach to address General Data Protection Regulation (GDPR) concerns raised in a European Court of Human Rights (ECHR) ruling.[11] This collection activity relied upon machine-learning decisions to deliver lawful-intercept implants to only specifically constrained IoT embedded-device endpoints associated with legitimate intelligence targets. Implant delivery to designated targets was based on an algorithmic decision that occurred entirely without manual intervention, so that minimization for legal purposes could be assured before any human in the loop initiated a collection event.

The initial document leaks involved a routine audit for algorithmic transparency, in which decisions of the machine-learning infrastructure were subject to interrogation, to assure alignment with POSTHARVEST' ethical principles.[12] While the POSTHARVEST program passed under all test criteria, a proposed revision was described in which the algorithmic change baseline could be hardened against potential adversarial learning influence. The hardening revision leveraged new commercial research, developed in large part out of the unique, emerging Silicon Valley successor firms of the Austin Hub, and had been funded by a block award administered through the Department of Defense (DoD) Joint Artificial Intelligence Center (JAIC) via several major US universities. Multiple Austin Hub firms involved in the project were also found to have been signatories of the Mavenite Declaration, in which a group of likeminded researchers forswore involvement in any AI research associated with military application.

8 Sandra Erwin, "Air Force to Award Contracts to Lockheed Martin, Northrop Grumman for Future Missile-Warning Satellite Constellation," *Space News, May 4, 2018, https://spacenews.com/air-force-awards-contracts-to-lockheed-martin-northrop-grumman-for-future-missile-warning-satellite-constellation/.*

9 Garrett Reim, "US Air Force Looks at Using F-35 as Ballistic Missile Interceptor," *Flight Global, January 17, 2019, https://www.flightglobal.com/news/articles/us-air-force-looks-at-using-f-35-as-ballistic-missil-455100/; "Special Mission (PM2)," US Navy's Military Sealift Command, https://www.msc.navy.mil/PM2/.*

10 For earlier discussion of the Westphalian-Plus concept, please see *Risk Nexus: Overcome by Cyber Risks? Economic Benefits and Costs of Alternate Cyber Futures, Atlantic Council, Zurich Insurance Group, and the University of Denver, September 10, 2015, https://www.atlanticcouncil.org/publications/reports/risk-nexus-overcome-by-cyber-risks-economic-benefits-and-costs-of-alternate-cyber-futures.*

11 For the record, it should be noted that the program described here and the associated cover term are entirely notional. The concept is based, in part, on discussion by the author with industry cybersecurity researcher(s) with extensive experience in machine-learning disciplines.

12 Seth Flaxman and Bryce Goodman, "European Union Regulations on Algorithmic Decision-Making and a 'Right to Explanation,'"(paper presented at the ICML Workshop on Human Interpretability in Machine Learning (WHI 2016), New York, June 2016).

The parliamentarian and several political-coalition supporters sought to use the POSTHARVEST disclosure to bar Austin Hub and other firms with US offices from EU markets, and to impose large fines on successful businesses. While ostensibly for human-rights concerns, over time similar actions evolved largely as an economic decision, in the hopes of creating protectionist barriers that would spur EU competitor developments in AI research. Since the 2000s, such innovation has not come to pass.

## COUNTER-CYBER OPERATIONS IN NO BOTS' LAND

Increasing proliferation of hostile intrusion sets, proxy actors, and sponsors reached a nearly overwhelming tipping point. Thus, a sustained optempo of counter-cyber operations requirements emerged, but the unsuccessful attempt to relay these narratives in Western media led to serious misunderstandings, and regrettable patterns of retaliation and escalation.

The lessons learned from these early efforts led to more sophisticated concepts of operation. Now, countering options occur both in cyberspace and across domains, employing a mix of conventional and covert actions, as well as diplomatic gray influence, and technical messaging. The latter, involving the deliberately tailored scope of targeting, choice of tools, and selection of effects across specific campaigns, is intended to communicate as clearly as possible, as much with the wider cyber-threat intelligence ecosystem as with specific competitor decision-makers. This ecosystem has become an ever more relevant channel for signaling as the expansion of non-US, and non-Western, commercial intelligence providers and consultants continued throughout the 2020s into a market that outgrew even the most optimistic of estimates authored at the start of the decade.

Concurrently, adversary learning under fire has created more resilient, distributed, and agile problems. The counter-cyber fight thus plays out in an unending exchange where advantage is all too often sought, weighed, lost, and regained on a week-to-week patch cycle to the next basis across an ever-proliferating range of infrastructure sectors, key enabling technologies, and business models.

The future technology environment has also offered adversaries new advantages, which have accelerated adaption under fire. The industry-wide shift to DevOps practices, including continuous update cycles, has increasingly offered a more tightly coupled, secure development lifecycle and faster remediation of security vulnerabilities once identified. However, certain changes have equally benefitted the attacker, such as: the increasing elimination of traditional distinctions between test and production environments; spreading developer cultures, which treat software releases as being in permanent beta; and the standardization of coding outputs in ways suitable to quality-assurance evaluation by automated test-harness constructs. Offensive capabilities targeting higher-order infrastructure above the level of the endpoint device, once considered the relative hallmark of more sophisticated intelligence-service-influenced adversaries, have proliferated widely as a variety of intrusion sets naturally observed the benefits offered by actions on objectives across router, tower, mesh, and backbone-level connectivity solutions.

The proliferation of targets and the expansion of the attack surface create multiple double-edged swords. As adversary options increase exponentially with the landscape of potential accesses growing denser, a counter-cyber operations element requires a similarly more extensive inventory of viable exploits, delivery techniques, and payloads. Often, these capabilities must be uniquely tailored to the adversary's victimized target environment, as well as to the capabilities stack that the hostile intrusion set has employed. Not only are labor and other procurement-related costs higher for Western cyber commands, even when capabilities may be developed internally through DIB or other contractors, but offensive programs conducted under democratic oversight also incur fundamentally greater overhead from multiple additional sources. Responsible offensive cyber-operations programs subject their capabilities to pre-deployment quality-assurance tests, as well as legal review.

The adaptive chase across a proliferating range of environments and technology solutions imposes additional cost on the countering service. While adversary operators can afford to incur collateral damage resulting from unfamiliarity with the target, countering operators are much more constrained—particularly where additional political sensibilities, or other protected characteristics regarding the adversaries' victims, must be taken into account. These dynamics will, therefore, demand that Western cyber commands organize to allow staff to develop a degree of specialization based on targets, or at least create other education and training mechanisms to cultivate and communicate the kind of operational experience that will allow for a subtler touch in the planning and execution of countering options within unique operating environments. Additional bureaucratic pressures created by such specialization, and attending certification, may greatly complicate the flexibility of talent

and process that may be needed to sustain pressure on an adaptive adversary that will inevitably learn, through repeated contact iterations, the types of innovation required to move beyond the scope and reach of the countering elements' currently constituted organization, authorities, and specialized experiences.

An even more serious scandal arose when a Kenyan cybersecurity startup found implants tailored to target mobile devices running a Red Crescent-affiliated app. This app sought to provide medical advice and treatment support to potentially vulnerable populations, as part of a program to track and contain emerging hemorrhagic fever infections. The app had been pushed for adoption by community-service groups following mass-casualty outbreaks impacting multiple African cities where refugees from the intractable Democratic Republic of Congo conflict had fled. The implant, dubbed "SICKCALL," was found to incorporate extensive anti-reverse-engineering features, and the Kenyan startup's founders attributed it to an unknown "Five Eyes" service in social media interviews that later went viral.[13] The lack of information about the implant—in part due to the small number of samples that could be acquired in the wild, as a result of apparently tight restrictions on activation criteria for the secondary payload dropper—led to rampant speculation throughout the hacker community.

Months after the initial headlines, a Western firm found that the SICKCALL implant trigger was tied only to specific instances of the app distributed through certain third-party app stores that lacked code review and signing functions of legitimate mobile-distribution channels. These suspicious app variants had themselves been earlier Trojaned with an entirely different malware variant. This original malware was found to be derived from an adapted variant of the GoldPage commodity crimeware family, which had been previously seen targeting pan-African mobile-finance apps commonly used by non-banked populations.[14] The Trojaned devices were incorporated into a peer-to-peer, takedown-resistant botnet. Researchers found that geolocation-service cloud infrastructure abused by this specific GoldPage botnet had been purchased by individuals designated under terrorist-finance sanctions, due to association with the Islamic State of Iraq and al-Sham (ISIS)-like organization known as Brotherhood of the Lakes and Valley (Jamaeat al'Ikhwan fi Albuhayrat Walwadi / Confrérie des Lacs et de la Vallée).[15] Briefings on the group's background by Saudi external-intelligence services suggest that the GoldPage activity is linked to exhortations for prospective shahid recruits to become infected with the disease in order to travel to major Western targets, including the Vatican and Christmas markets in France and Germany. The compromised Red Crescent app provided geolocation targeting that the terrorist organization's planners leveraged to maximize the chances of suicide-operation candidates to come into contact with disease-carrying local populations during initial asymptomatic incubation periods, in order to maximize potentially viable travel windows and minimize the probability of detection of the shahid carrier by bio-surveillance protocols in place at international airports.

## INSIGHTS

The paradox thus created—in which the deterrent credibility of US capabilities is derived from use, while the potential advantage in achieving tactical and operational success remained from the undisclosed nature of innovative exploitation and effect options—will create a constant tension for planners and operators.

Great-power competitors have exploited the West's divided internal responsibilities for sovereignty, security, and control of cyberspace. These adversaries have become adept at exploiting the seams between organizations and authorities created by a free and open Internet, with government presence constrained by the constitutional traditions that separate foreign from domestic considerations, military from law-enforcement roles, and official from non-governmental actions. These tensions will not be easily resolved as the West continues to struggle to contest hostile pressure below the threshold of armed conflict. However, innovative approaches are needed, in which executive, legislative, and judicial agreement can be reached to enable sustained aggregation of talent, budget, and mission execution against threats about which impacted stakeholders have reached a consensus.

These dynamics shall be exacerbated by changing technology stacks that will reshape the virtual terrain in which cyber operations are conducted. The continuing shift to ubiquitous computing across ever more pervasively distributed functions of society and daily life will change the fight in ways that make this more intimate to the population as cyberspace continues to evert, leaving the conceptual and physical confines of an abstracted invisible network and embedding across the

13 Notional cryptonym.
14 Notional cryptonym.
15 Notional threat group.

host of devices, services, and day-to-day interactions with objects that define the physical, built environment. These will include: ever more mediated interpersonal interactions between family and friends, and between communities and their beliefs; deeper influences on the individual through new wearables, as well as therapeutic and preventative medical technologies; augmentation to restore and extend sensory perception and memory; and an increasingly complex fusion of online identities with the physical person through dress and body modification.

Substantial concerns will almost certainly continue to surface regarding the overall strategy of persistent engagement. International relations evolve slowly, in both theory and practice. There is a profound gulf between even the closest of allies in understanding the perceptions, equities, and remedies for the trespasses of hostile actors against sources of national power. This gulf will undoubtedly continue into the future as conceptions of power and its purpose remain divergent between US and continental thinkers and policymakers, to say nothing of the wider number of emerging powers. Yet, despite this gulf, key relationships between allies will remain vital to pursuing countering objectives. The development of effective working constructs in which operations can be pursued within jointly understood boundaries—in analogue akin to the Proliferation Security Initiative agreements—will likely command the weight of diplomatic and deconfliction efforts for some time to come.

These relationships must also be extended beyond traditional partners to encompass the private sector—not merely through trite lip service given to public-private partnerships, but through what may seem quite radical thinking about the changing nature of sovereignty in this new domain. Private players will take on new roles in these constructs, from intelligence providers to enabling partners to acting through their own unilateral offensive and hack-back operations. In many cases, these possibilities will require uncomfortable conversations, difficult adaption, and a clear-eyed look at the hard realities of the contemporary and future operating environments to address the domain as it is, rather than through idealizations of a lost world that may never be regained.

Great-power competition will necessarily reshape Cold War-era legacy alliances in ways that are currently difficult to estimate. These tensions that arise out of economic competition create substantial opportunities, and no small incentives, for economic espionage even among erstwhile friends. Cascading exits from a unified Europe may render this among the most complex, contested landscapes of cyberspace, should existing impulses toward broad regulation as an instrument of cross-border control be leveraged aggressively through "enforcement" mechanisms, relying upon the unique advantages that actors may gain through cyber espionage.

Competition, sometimes involving sharp elbows among cousins, will further exacerbate the long-standing, and unlikely to be resolved, issues of lawful intercept, warranted access, and encryption backdoors. The proliferation of increasingly robust encryption, covering ever-wider ranges of individual and corporate communications, will almost certainly drive calls for bureaucratic solutions attempting to mitigate the inevitable abuses and unknown downsides. However, in a world under constant contact, such "easy" solutions—aimed only at the entities that would comply with government mandates—might well rob the cryptologic enterprise of the drive, resourcing, and sustained focus required to ensure the ability to break adversary codes regardless of algorithm, implementation, or environment. The need to assure this capability dominance, both in relative and absolute terms, may be considered a sine qua non pillar of the cyber-warfare domain.

## IMPLICATIONS

- (Near-Term) Renewed and sustained economic espionage campaigns at escalated pace, intensity, and scope
- Continued incentives for commercial disclosure of unique Western cyber capabilities observed in the wild, facilitated by new researchers and emerging-market firms potentially influenced by hostile foreign intelligence services, in ways both subtle and shockingly direct
- Potential for hard decisions trading off vulnerability in key targets and critical infrastructure to retain high-value capabilities for future responses and counter operations
- (Long-Term) Potential for altered relationships with historic allies and partners in cyberspace as states face political realignment in Europe, collapsing population demographics, and effects of serious budgetary crises
- Novel aggregations of talent, visibility, and risk appetite leading to crises with previously unknown actors and unanticipated capabilities, which upend key defenses, intelligence capabilities, and defensive investments with limited warning and outsized impact

# SCENARIO 2—AI and Insecurity for All: The Future of Cyber Conflict

Dr. Chris Whyte

## SETTING

The logical result of AI, at the heart of any major evolution of practice and strategic thinking on cyber conflict, is an international AI arms race centered on discrete military functions. Even narrow AI will have profound impacts at every level of cyber confrontation, from speeding up and creating new attack vectors to highly sophisticated target identification and discrimination. At the high end, it will empower nations to achieve their goals in new and innovative ways, unencumbered by the R&D and physical development, or the laws and restrictions, of historical weapons-systems development, thus sparking a race to explore the art of the possible. Even more challenging is that, unlike historical arms development, nonproliferation constraints will be almost impossible to create or enforce.

## KEY TRENDS

Changing Security Landscape: The continuing integration of narrow AI in a wider array of daily activities alters security relationships. The manner and degree of this alteration depend on the source of this AI—nation-states or the private sector.

Towers of Babel: The use of AI-enabled cyber capabilities will create trust and coordination challenges, the scale of which will be determined by the extent of the Internet's fragmentation along sovereign lines.

## SCENARIO

AI technologies are poised to revolutionize global society. At the same time, new information technologies diversify and fragment existing sociopolitical and security infrastructures in a manner that increases the importance of the myriad digital interactions defining daily life in future conflicts. In this new landscape, the struggle for control of and access to foreign systems will pivot on the degree to which discrete abilities to operate online can be modified, automated, and made smarter via the application of AI techniques. While other revolutions in technology (and the social understanding thereof), politics, and economics will undoubtedly affect the manner in which cyber conflict is fought, AI will—arguably more than any other driving force—dictate the boundaries of possibility for combatants online. In effect, AI could make it easier for a wider range of actors to increase the speed of interactions (e.g., offense, defense, espionage) and reduce barriers to entry. This scenario overview describes the opportunities and challenges bound up in AI-augmented cyber capabilities, before outlining different possibilities for how such advances might affect global conflict conditions.

Artificial intelligence constitutes a cluster of technologies that, either individually or in tandem with other technologies, allow machines to more effectively shape and responsively be shaped by their environments. In its simplest form, intelligence in machines is anything that moves a system beyond a base ability to process information and respond with predefined program instructions. Though AI, in its simplest sense, is a function of micro-behavioral programming, the result of machine intelligence is something beyond the structured algorithmic processes that characterize sophisticated computer programs. In the field of AI study, these systems are commonly categorized as either "narrow" or "general." Narrow (or "weak") AI means the implementation of intelligent technology so as to massively improve upon human abilities to perform specific tasks. While general (or "strong") AI—which is broadly held to be a machine intelligence capable of performing any task a human could—is assumed to be still some decades away, this paper is concerned with these narrow systems that dramatically extend the boundaries of possibility for tasks traditionally performed along specific lines by humans.

The basket of technologies under discussion is often said to include any developments that allow machines to move independently (e.g., robotics technologies) to sense the environment, and to learn from it such that case-specific responses are possible. In reality, this last category of technologies is the one most commonly referred to in conversations about AI, and is the most relevant for any conversation about AI and cyber conflict. Technologies that allow a machine to learn are

those that enable the leap beyond structured responsiveness, i.e., to pass the Turing test, which determines if a machine intelligence can be distinguished as not human. These technologies—machine learning, natural language processing, automated reasoning, and knowledge representation—enable smart systems that work from an existing understanding of the environment in which they operate, adapt outside knowledge probabilistically to an environment, and use neural networks to test and generate all new knowledge about an environment.

## AI AND DYNAMICS OF CYBER CONFLICT

Technologies that help machines learn and perform discrete tasks by applying expertise of a level equivalent to or greater than what would be possible with human operators are likely to increase the speed of interactions in cyber conflict, and reduce barriers of complexity that currently pose a significant issue for attackers and defenders alike. In doing so, it will democratize cyber conflict and create more, and more complex, sets of actors within the domain. Perhaps most notably, AI is likely to underlie the production of a new class of persistent threat tools (and, resultantly, actors) that can penetrate foreign systems and adapt to countermeasures more effectively than is generally possible at present.

Perhaps more significantly, an enhanced ability to rapidly shape approaches to fit the contours of a smart environment is also likely to portend a further blurring of the lines between cyber and information operations. After all, smart and highly adaptable automated intrusion instruments that holistically consider target ecosystems are well placed to adopt courses of action that, in addition to more effectively compromising enemy systems, trick defenders and force them to question the nature of their defensive efforts. The obvious implication of developing such capabilities is a parallel rush, by both governments and private industry, to produce better AI-driven defensive tools. Such systems (like the Autonomic Intelligent Cyber Sensor) already exist and are destined to get better, both as technologies advance and as new forms of smart cyber threats are realized.

Strategically, the prospect of an arms race focused on AI tools that enhance cyber-conflict capabilities is worrying on several fronts. Broadly, the added potential scope and speed of AI-enabled cyber operations present a challenge for investigators, insofar as the relevance of innumerable, persistent actions will be difficult to ascertain. A highly advanced spearphishing campaign that leads to the compromise of defense-contractor systems today, for instance, might be relatively simple to reconstruct. An AI-driven effort that uses social media interactions to identify users more likely to be guilty of poor cyber hygiene, so as to launch a spearphishing attempt from diverse sources, is likely to be much harder to identify. Added complexity means added time to respond effectively, unless similarly sophisticated defenses can be brought to bear. Such defenses are likely to benefit from AI advances in a less acute fashion, even where successes are had, as the task is more inductive than is attacking. Scaled up, particularly where targets are not only (or even principally) in the public sector, this equates to an exacerbation of the challenge of target hardening at a national level. This will also shift the incentive structure for illicit behavior, as the cost-benefit ratio increases with the improved likelihood of success.

The problem of complexity also manifests, perhaps even more worryingly, in the development of the IoT. The advent of driverless cars, within-body medical implants, and accommodating infrastructures (among many other examples of the burgeoning IoT) presents new vectors for attack for both criminals and politically motivated operators. Particularly where cyber conflict is often an adjunct modifier of rising tides of political-warfare efforts, the expansion of the IoT—in combination with advancing smart-intrusion capabilities—may enhance possibilities for the coercion of individuals and institutions beyond the state. As recent scholarship on the value of cyber operations to information warfare has suggested, this is meaningful for state security considerations, because such societal actors—e.g., prominent politicians, celebrities, or experts—are often critical enablers of the normal function of ideational and economic marketplaces.

## THE BYZANTINE NATURE OF AI-DRIVEN CYBER CONFLICT

The likely result of added complexity from AI augmentation of cyber-conflict processes is a reduction in the fault tolerance of both national socio-political and military systems. While there is uncertainty stemming from the attribution challenges inherent in online interactions, the addition of AI is likely to make such uncertainty permanent in future cyber conflict. If such instruments are able to rapidly adapt their approaches to operation at the level of overarching campaigns, the natural outcome is a diminished ability to assess sources of failure along the kill chain. In reference to the paradigmatic Byzantine Generals' Problem, a game in which armies are forced to communicate in

order to carry out a successful attack, this outcome becomes synonymous with a strategic posture where the inevitable compromise of dispersed systems seems arbitrary—at least in the context of those intrusions deemed strategically meaningful.

"Reliable computer systems must handle malfunctioning components that give conflicting information to different parts of the system. This situation can be expressed abstractly in terms of a group of generals of the Byzantine army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach agreement. It is shown that, using only oral messages, this problem is solvable if and only if more than two-thirds of the generals are loyal; so a single traitor can confound two loyal generals. With unforgeable written messages, the problem is solvable for any number of generals and possible traitors."[16]

This dynamic has major implications for both the prospect of deterring hostile action in cyberspace and for the dangers involved in the employment of cyber operations in crisis scenarios. On one front, the ability of foreign adversaries to design smart attacks that variably force Byzantine faults—and can otherwise be crafted so as to send deceptive signals—makes static assumptions about the deterrent value of either defensive or punitive postures unsafe. Certainly, it is possible for punishment to successfully shape the actions of foreign belligerents around specific issues and points in time. However, an arms race centered on smart instruments that can rapidly employ effective simulative and dissimulative techniques for tactical gain—informed by strategic conditions—naturally suggests that assessments of deterrent success are increasingly likely to lack staying power. On the other front, those carrying out cyber operators under crisis circumstances must grapple with an intensification of various psychological dynamics. Are intrusions during such periods a deviation from "normal" patterns of persistent engagement in cyberspace or do some suggest an escalation? Particularly where cyberattacks lead to unusual outcomes, should operators write intrusions off as duds, or assume some kind of lateral threat? Where AI augmentation is at play, people may be increasingly incentivized toward opting for the latter option.

## FUTURE AI-DRIVEN CYBER CONFLICT

The dynamics of future cyber conflict augmented by smarter, automated AI instruments are themselves dependent on external conditions. In other words, AI is likely to factor into different broad developments in the role of cyber conflict by state actors, based on the conditions of its evolution over the next few decades. Here, this paper describes four future "worlds" (scenarios) in which the significance of AI differs in the context of broader geostrategic dynamics. It suggests such significance emerges primarily from the interaction of two exogenous sets of developments: the degree to which AI research and development is driven by state security apparatuses (inclusive of closely affiliated private defense partners) or private industry; and the global condition of the Internet as more or less fragmented along national lines.

In Worlds 1 and 2, state-driven development of AI instruments for waging and defending against cyber conflict occurs in the context of different structural evolutions of the Internet. In World 1, the Internet several decades


16 Leslie Lamport, Robert Shostak, and Marshall Pease, "The Byzantine Generals Problem," *Programming Languages and Systems* 4, 3 (1982).

from now is no longer a truly global construct, and is instead split between the enduring open Internet of Western societies and the curated gardens of authoritarian states like China, Iran, and even semi-democratic nations like Singapore. In this future, cyber operations are intrinsically tied to the societal value proposition of the competing models of connectivity, and the AI arms race, clearly driven by state interests, is politicized as an instrument of subversion. In this scenario, AI plays even more of a game-changing role than in other potential futures, because development is held close to the chest by stakeholders in distinct, competing ecosystems of social, economic, and political operation.

By contrast, World 2's vision is that of state-driven AI development in a world where private-industry interests and Western concessions to a hybrid multilateral, multi-stakeholder governance order have maintained the Internet as a global construct relatively free of Balkanization. Here, though states are in the driver seat, the less politicized employment of AI and shared problems with AI-enabled cybercrime open a space for international coordination on standards and thresholds for the automation of cyber operations. Despite rising complexity, the development of norms based on international legal precepts helps states develop somewhat effective deterrent postures for cyber conflict.

In Worlds 3 and 4, private industry takes the lead in developing AI technologies useful to cyber offense and defense. Here, the question of how significant AI is to future cyber conflict is really one of sovereignty and access control. In World 3, an open global Internet combines with distributed sources of AI development and incorporation into cybersecurity tools to produce a mini-fragmentation effect, as the best way for vendors to offer protective services is through the development of proprietary, limited-access environments. This effect is particularly pronounced as societal "off-gridding" becomes an increasingly common choice across the West, and as cities become more significant political units than state, or even federal, entities. For private industry, increased vulnerabilities emerging from the expansion of the IoT and off-the-shelf smart tools for more effective hacking mean that commercial success often entails promising an active role in preventing external interference with services. Thus, though the task of states in developing their cyber arsenals in tandem with (or by investigating the products of) private industry remains much as it is today, the proliferation of custom solutions to AI-driven digital challenges limits the ability of states to cooperate with peer competitors.

World 4, where the role of private industry in developing AI instruments firmly clashes with the divided nature of the Internet, compounds this problem and places responsibility for the integrity of information services and routing functions beyond the hands of states in the public eye. Thus, the tactical challenge for states using AI-augmented cyber capabilities for conflict purposes in this double-fragmented world is the addition of imperatives placed directly on the shoulders of private industry by popular opinion. Given principled support for the integrity of one system over another, Internet service providers (ISPs) and other developers pose a sovereignty challenge for states in their ability to interdict military and intelligence use of their platforms.

## IMPLICATIONS

- (Near Term) Potential for new classes of persistent, autonomously adaptive, cyber capabilities
- New approaches to social engineering stemming from an increasingly blurred line between influence and cyber operations
- New sources of vulnerability with advanced telecommunications and IoT devices
- (Long Term) Increasing probability of an AI arms race
- Rising opportunity cost as the need to spend more on hardening targets diverts funds from offensive activities to defense

# SCENARIO 3—Systems Apart: Filtered, Throttled, Poisoned, or Collected?

## The Global Split in SOCMINT and Data-Flow Structures

Dr. Nina Kollars

### SETTING

Political warfare within fractured and competing network systems creates new risks and opportunities. Networks have begun to fracture in several ways: commercially, as companies like Apple and Google seek to lock consumers into their ecosystems; culturally, as domestic subgroups with differing ideologies seek platforms and communities that reflect their own views; and governmentally, as authoritarian regimes seek to control their online environments to keep their populations in line. Across these fractures, cultural norms and values will diverge further, while also creating new battlegrounds of influence. These dynamics and ever-shifting mutations will have profound impacts on the threats the like-minded nations face and the opportunities to achieve strategic goals.

### KEY TRENDS

Rise of the Splinternet: Through expansions in country-level regulation, a thinning marketplace for social media through competition, and increased government interest in the capacity for political influence through social media, the public-opinion space of the Internet has developed its own kind of geography, one based on friction and the blocking of data flow across boundaries.

Live a Life Online: The global appetite for a social Internet in the consumer's back pocket has become a target too tempting for political actors to ignore. Social media intelligence (SOCMINT) grows as a mechanism for state power projection and domestic political influence.

### SCENARIO

A decade-long staring match between democratically allied countries on the one side, and their own private sectors on the other, has finally begun to reach a conclusion. It took only one direct social media campaign from Russia (posted simultaneously to every known social media platform in every possible language) to resolve the internal standoff and usher in a coherent "democratic" model of social media control.

That catalytic Russian campaign, now dubbed the "Righteous Security" movement, consisted of a direct and open invitation to emigrate to Russia from the leader himself—to "live safely inside the republic as new Russianites with truly secure borders." The Russian leader's invitation was never determined to be authentic. There wasn't even enough time to dissect that, let alone to attribute it. That didn't matter; the effect was utter pandemonium. It was one thing to subtly disinform and divide unthinking lazy tweet/gram/status updaters, but another entirely to—so directly—use a public against its own government. It was pure passive-aggressive, state-on-state intimidation of a kind so bold that its virality could not be contained. The thirty-second clip took fewer than thirty-four minutes to reach tens of millions of views, followed by no fewer than one hundred thousand memes of every shade—humorous, racist, hyperpatriotic, and lewd.

Virality proved itself to be the enemy it was. There was no need for bots; humans did well enough on their own. Better than any dreamed National Security Agency (NSA) cyber exploit, the virtual became the physical in less than a day. With people deeply divided and primed for outrage (real or otherwise), violence began as false rumors spread of mobs gathering to take the deal. Homes were ransacked and looted as accused "bear lovers" ran for their lives.

Political leaders didn't dare contact their Chinese counterparts, but echoes of "早就告诉你了" ("I told you so") still filled the deafening diplomatic silence. In the triad of industry, government, and citizens, the Chinese had clearly decided to first route international data flows through their own systems before they reached the casual media user inside China. Whatever a free and open Internet meant, the answer for the rest of the

world was to wrangle the beast, but not exactly in the same way China had. When it finally ended, too many days later, there was nothing left to do but bring Silicon Valley's volatility machines to heel.

That was the tipping point. No longer shy about "damage to an innovative startup marketplace," democratic alliances no longer wondered academically whether their stability was endangered by social media. The question was not if "socmed" disrupted publics, or even how to limit the disruption. Instead, it was finally time to become clever. If the Internet influenced the social, then it was obviously a tool for politics in the international system. The question was: how can virality be controlled and manipulated for the stability of allies and create headaches for the adversary? All countries—aligned, democratic, authoritarian, or otherwise—asked the same questions. How are foreign entities engaging with the social media industry? Through which platforms, and who owns them? The answers, and what countries did with that knowledge differed markedly.

What academics used to call the "fractured" or "bifurcated" Internet has revealed itself to be far more interesting. Missions of public influence—mostly domestic and international—are now the standard in the social media wash of the citizen's day. More than a decade ago, under government and market pressures, the epidemiological vectors of infection and virality became fodder for regional and state efforts to shape and project political power.

SOCMINT analysis is now the centerpiece of all good startups in both Silicon and Shenzhenicon Valleys, but the structure is fundamentally different. Two essential models emerged: filtering and attenuation.

## FILTERING

Countries with difficult regime stability were no less subject to the emotionally disruptive nature of dense social connectivity. Those regimes opted to filter early on. That is, they focused on the platforms and hardware, placing themselves between the international deluge of destabilizing "infor-emotion" coming from the international echo chambers. Careful sorting and sifting of what should and could be understood by their own publics have become automated. The citizens inside exist in a well-tailored information environment that reassures its hardworking, busy city-dwellers that the people's place in their society is healthy, and that they are exemplars to the world of the superiority of their social order. This is all supplemented with the state's well-established, segmented internal systems that route data through the state's impression filters to ensure the careful selection of potentially damaging thoughts, and to amplify order-producing impressions.

China, through an inertia of too-well-structured thinking, has created a tightly coupled system that is nearly brittle, causing anxiety for its planners and trigger-finger nervousness for its cyber-defense teams. The early onboarding of deep neural-networked learning systems that can sort through the morass of data flows between citizens, and from the outside, has been under attack since first activated. The first mover advantage too quickly became the first to implement and, ultimately, the first to be attacked. Thinly veiled state-on-state manipulation of images, audio, video streaming, and written content is rife within the network. Regional security regimes and competing adversaries find the tightly coupled system, with the not-yet-desensitized public inside, has shifted to attacking algorithms, trying to force the AI filter to learn the wrong things entirely. Adversarial artificial-intelligence techniques and counter-AI software are openly traded on gray and black markets.

## ATTENUATION

Aligned democratic countries—i.e., those that share fundamental democratic values, but are also the central producers of private-sector platforms—came up with a slightly different design. What is now commonly referred to as the "carrot and two sticks approach" of direct investment coupled with regulation was implemented, along with severe costs for noncompliance. Churn in social media marketplaces, repeated data-breach environments, and the inability to successfully monetize the secondary-information market like the heydays of the 2020s have turned from data-compliance requirements to full regulation on the government side, and willing cooperation for the remaining social media systems on the development side. Several years of the inability to control social media virality—and, therefore, stock value—have given way to exhaustion for private-sector investors and boards seeking stability in the arms of the government. Public television, long since defunded, is reborn and funded as public social media.

This loosely coupled system, completed with front-end viral governors, remains vaguely heterogenous and organically configured across the aligned countries still enamored with some notion of a "free and open Internet," with some elements of the early Silicon Valley multi-solution incubator characteristics left. The viral governor doesn't seek content; it simply seeks a

footprint. If the systems sense virality, the throttling begins. A slowing friction ensures that thoughts are permitted to spread, just not too fast. Sometimes, the throttling produces waves of information paced just in time for an informed public. It's just enough for policymakers and politicians to get in front of the wave. Perhaps to ride it, or even shape it. A whole secondary market in beltway pundits and election campaign managers rises up to reach deep into surfing metaphors and ocean patterns for new tactics and techniques, giving birth to new lingo: there are "Jakes," "Hodads," "Bennys," "taking headers," "kicking out," or getting "locked in."

For the private sector these days, new platforms are only half of its monetization scheme, since the great social media bot.com bomb (version 2.0 of the dot.com bust of the late 1990s) wiped out the vast majority of those left gasping on persistently renegotiated venture-capital dollars and draconian mergers-and-acquisitions processes. Since then, the Five Eyes, NATO, the Internet Corporation for Assigned Names and Numbers (ICANN), and myriad standards entities have intervened to stabilize an intensely volatile system. In its place, full governmental implementation of front-end development of data-collection formats aids countries' efforts to predict and shape the rate at which public voices can be heard.

Reluctant to filter, countries opt for throttling, and more importantly, collection. That was the final deal struck. The real trade-off for public funding of social media was the right to know who, when, and how the public was connecting at the front end, instead of trying to understand it at the back end. That intelligence was then recycled into the international cyber teams tasked with locating and neutralizing noxious non-state threats to the Alliance and its security.

For a short while, there was protest. The original security-versus-privacy debate evolved into a stability-versus-censorship debate, with vitriol leveraged along nearly every possible political line. In the meantime, the public lost interest, as it had every other time. It largely quit out of rage but then, following a few days of "fast or purge" on the platform, inched quietly back and eventually returned to previous fervor levels. Regulators assured journalists and human-rights organizations that separate dark-web spaces would go untouched, but the public capacity to damage itself was finally declared a public mental-health issue, and virality was declared an official menace to the security of the nation.

The effect was exactly as espionage agencies had dreamt. There was an illusion of heterogenous free and open spaces for discussion, with front-end access to records, and how that data should be sorted and stored. The throttled system, however, had its own attributes. Rather than a tightly coupled system in which cascading effects could create second- and third-order immediate effects that could get out of hand, this loosely coupled panoptic system resulted in a disaggregated, and remarkably slippery, environment. The Chinese became the masters of the metric, constantly testing and re-testing the continued influence China might have over outside perceptions of its "panda" face.

## IMPLICATIONS

- (Near Term) Virality on social networks is increasingly understood as a threat to states' political stability
- Some states will abuse virality to disrupt political processes around the world. In reaction to these efforts, social-media-saturated states will eventually try to limit the influence of social media on domestic political stability through regulation and taxation.
- Failing to see success with this effort, states will then try to implement actual front-end digital and physical controls on social media firms; this control will manifest as either throttling or filtering, depending on the state's perception of risk from viral social media
- (Long Term) What was first viewed as a poison is eventually weaponized with remarkable nuance; the purpose of throttling and filtering will begin to shape offensive military strategies as a mechanism for shaping great-power politics through all phases of potential military conflict

# WILDCARDS

While this report provides a chance to dig through several alternative future scenarios, these are by no means the only compelling possibilities. Below are several others generated from the ideation event that could provide the basis for further scenarios in their own rights.

### *Chaos in China*

Targeting of trade secrets remains driven by key enduring factors, including: the aging Chinese population and the associated need to steal biomedical advances that cannot be duplicated within corrupt, connection-driven university and industry research structures; the breakdown of trust in ever more manipulated official statistics, leading to cratering foreign direct investment; a constant demand for agricultural and energy-technology innovations to combat the ever-present urban-rural imbalances in prosperity and quality of life; and the rapacious need for inside information to drive advantage in negotiations over the never-quite-stable Belt and Road dream. Feeding the force required to execute looting on such an obscene scale is a complex network of Ministry of State Security and People's Liberation units, reorganized with some regularity as cover designators are burned and new mission-focus areas emerge to command specific interest and, therefore, internal factional advantage in aggregating talent and tooling for dedicated purposes. These units are, in turn, supported by a bewildering array of contractors, suborned and subverted technology firms, and capabilities acquired through underground criminal marketplaces collectively considered under the analytic concept known as "QUARTERMASTER."

### *The New Frontier*

A variety of macro trends is shaping cyber strategy and societies' support for cyber operations. This includes an economic decline resulting from a combination of the collapse of the global middle class, high debt levels, and the Fourth Industrial Revolution, leading to large-scale unemployment and underemployed white-collar workers globally, which has impacted states' ability to generate resources (guns vs. butter). Global inequality has skyrocketed, creating a new super class.

The city has risen to become the new political unit as increasing urbanization focuses most attention on more immediate political concerns, including networks. Corporations have taken the lead and, given resultant government decline, new companies that mix cybersecurity, insurance, and paramilitary capabilities are coming to the forefront to offer hack back and other services. Essentially, new actors are taking the reins to protect individuals, cities, and firms as governments remain underfunded, bound by legacy restrictions, and worried about escalation. Many of these hack backs and other services respond to low-end attacks launched by underemployed workers looking for extra money and opportunity. This has, in effect, created a system of new city-states.

### *Luxury of Privacy*

The transparency that has come from ubiquitous social media use and widespread DNA analysis is shifting views on identity, cultural values, and societal concepts of privacy. On the one hand, individuals' own choices about privacy are becoming invalid as others take DNA tests and/or upload data about them online. People no longer have a choice to be private, and cannot control their own data. Only the very resourceful—either monetarily or in terms of certain skills—are able to shield themselves, and even then only to a certain extent. Meanwhile, ideas on issues such as race shift as individuals' genetic lineages are exposed, for better and worse.

These advancements are also changing how nations undertake strikes against criminals and threat actors, particularly when combined with medical advancements that expose those individuals to highly precise tracking using diabetic blood-pressure sensors and similar devices. The ability to target individuals so precisely has shifted how Western societies risk appetite for targeted killing. The certainty and precision strikes have increased the general public's acceptance of the practice.

### *Brittleness of the Gig Economy*

The sharing/app/gig economy steadily replaces traditionally state- and city-provisioned services with cheaper and more decentralized models. Over time, this erodes key infrastructure as it becomes underutilized and uneconomic, and as market forces drive local governments to turn to private alternatives. Buses, for

instance, have disappeared from most cities due to the number of ride-hailing services, bike-share options, and the like.

While this creates a highly efficient economic model, it creates unforeseen fragility as services lack depth and obligation. When a significant shock impacts the new ecosystem—either from an exogenous and uncontrollable event, such as a natural disaster, or from key nodes in the ecosystem, such as a few key apps, failing—the entire system becomes unworkable.

This manifests when a sudden earthquake hits a major city. Most ride-hailing drivers fail to come out as they seek to look after their own families or feel it isn't safe enough. After excessive price gouging, a few return, but not enough to move sufficient numbers of people. Bike-share assets quickly get used up and end up outside the city center as people flee to the suburbs. Without public-transport options, huge numbers of people become stranded. Society has lost all resilience, and careful social targeting allows attackers to cripple cities easily.

### *Trouble "Makers"*

A generation that has grown up in a "maker" culture, with an abundance of non-formal educational options, has reconceptualized traditional jobs, industries, and how they solve problems. At best, this means they no longer have a need for some forms of professional experts, as they are comfortable teaching themselves necessary skills and turning to the gig economy, meet-up networks, and crowdsourced answers for ways to address problems.

A darker manifestation of this culture is that many kids who grew up "swatting" gaming opponents look for more advanced ways to leverage institutional powers and capabilities to solve problems or gain advantage. They instinctively look for ways to pirate others' capabilities for their own—often destructive and potentially violent—objectives, with few consequences or accountability.

But, there are additional potential possibilities: this approach of leveraging others' (including state) infrastructure for their own needs could spurn a generation of pirates who create illegal (or, in some cases, semi-legal) business models that "piggyback" on digital infrastructure. This would involve penetrating a system, then using that access to sell services rather than to degrade, steal, or attack it. This creates a complex web of implications, not all of which are negative. Under some circumstances, pirates may end up unintentionally enhancing or improving the digital infrastructure they are pirating in order to make their illicit business more profitable and stable.

### *Who am I?*

Societies' concepts of identity and privacy have irreversibly shifted. As the general population becomes increasingly aware of its own—and others'—DNA data, some groups have become increasingly elitist about the purity of their DNA. For others, racial identity and cultural bonds have eroded as it becomes clear how interconnected parts of the population are; when everyone is special due to their genetic history, no one is. Concepts of nationality and identity shift radically. This rapid shift in cultural identity creates even greater rifts between those who embrace technology and progress, and those who feel threatened and left behind.

### *Cultural Divide*

China has successfully created its own walled garden, complete with its own undersea cables to and from key Southeast Asian countries, and even leads the world economically. The world is divided into open Internet and censored Internets, based on alliances and geographical proximity. The supply chain of technologies is divided according to trusted and untrusted pathways, creating serious shifts in economic growth in high-tech industries. US domestic firms are forced to make serious choices about where and what their technologies do according to these lines.

This emerges in geopolitics as a new source of tension between the West and the rest. For cyber operations (cyops), the fundamental clash of two visions of a transforming digital terrain has several implications. Most interestingly, it supports an underlying crisis of sovereignty wherein ISPs, backbone operators, and developers are both faced with the decision to support consumer interests over government interests and find themselves more acutely the gatekeepers of access to significant target infrastructure and populations. Devolution of authority for security to the regional and urban is inevitable in both free and controlled blocs, both of which see developing crises of state authority. The result for federal cyber operations is either inevitable mission creep and bloat, or the strategic retreat to prioritization of core systems in an environment of persistent engagement across the landscape of the national unit.

# CONCLUSION

The future of cybersecurity is uncertain, but these three scenarios highlight narratives and concomitant trends that could shape the strategic dynamic for years to come. In their discussion of changes to how contestation and competition happen in cybersecurity, the three scenarios highlight a deeper challenge for the national security enterprise: how to adapt legacy concepts, capabilities, and organizations to meet the challenge of a hyperconnected and rapidly changing world. While additional research and experimentation are required to define new operational approaches in terms of ways and means, this report begins that journey.

The analysis of these scenarios highlights strategic ends that the US national security community, along with key allies and partners across academia, civil society, and industry, must accomplish in and through cyberspace. These include

- actively defending open and democratic societies against exploitation and manipulation by authoritarian regimes and violent non-state networks that seek to erode the free flow of ideas and goods;
- working to rapidly identify, assess, and counter emerging cyber trends, without triggering inadvertent escalation or producing unintended spillover effects that corrupt vital networks or resources;
- increasing allied-state, partner-industry, and key civil-society interoperability as means to ensure rapid, more effective, and cohesive responses to attacks on open and democratic societies;
- creating cross-computational and cross-domain capabilities, including fusing offensive cyber infrastructure and information warfare and enabling both with new machine-learning techniques and automated decision-making, without violating norms at the heart of a democratic society; and
- restraining the growing weaponization of social media.

None of these strategic ends will be accomplished by the US national security in isolation—they require strengthening existing foreign alliances and partnerships with academia, civil society, and industry as well as organizing to forge new links. The scenarios each postulate an alternative future, but trends within each threaten the achievement of these ends.

### *Scenario 1—Great-Power Competition and A State of Friction*

The pace of cyber operations and the influence of these activities on areas outside of military competition, including the development of new economic hubs and businesses, demands changes to how organizations prepare and fight. Traditional dyadic deterrence through threat of overwhelming force is less persuasive, and adversaries regularly employ proxies to induce uncertainty and increase the cost of retaliation. Managing the risk of escalation in this environment demands clear doctrine and tight alignment between tactical, operational, and strategic leadership. Collaboration and capacity to coordinate with partners like allied states, industry, academia, and civil society become key determinants of success in whole-of-society defense operations. Strategic efforts by adversary states to fracture extant Alliance structures are more acute, and may require broader strategic engagement with close partners, beyond national security goals.

### *Scenario 2—AI and Insecurity for All: The Future of Cyber Conflict*

The increasingly rapid integration of machine learning and automated decision-making into cybersecurity operations and information warfare is tightening decision-making windows and reducing opportunities for deliberated human intervention. The defense of open societies will be complicated by a potentially fragmenting Internet with similar disruption to consensus norms on how to prioritize defensive and healthy machine-learning research over that which might contribute to escalation and more rapid cycles of aggression. This fragmentation will similarly impact the ability to drive operational integration of machine-learning and automated-decision-making technologies as research across states and the private sector may radically diverge.

### *Scenario 3—Systems Apart: Filtered, Throttled, Poisoned, or Collected?*

Internal political discord hampers efforts at whole-of-society defense against authoritarian

manipulation. The fusion of machine learning and automated-amplification loops in weaponized social media creates fearsome scale for even small injects. Schisms between the private and public sectors hamper coordination in combatting these social media campaigns and concomitant influence operations across other domains. Domestic political fragmentation and evolving institutions limit the agility of Western responses to adversaries as they utilize an increasingly connected global population as battlefield terrain—gathering information and deploying effects through social media.

As the character of the competition changes, it alters the ends, ways, means, and risks associated with cyber operations. The competition continuum at the core of the new Joint Integrated Campaigning Concept extends to the three interrelated layers of cyberspace, i.e., physical networks, logical networks, and cyber personas.[17] Great powers employ new ways and means across these layers, often beneath the threshold of armed conflict and executed via proxies, to gain a position of advantage. These states manipulate fog and friction to limit their targets freedom of maneuver. Many of the resulting strategies confuse, blunt, and undermine adversaries from within, blurring the line between combatant and non-combatant to obfuscate the very definition of war itself.

As these scenarios illustrate, technological change and evolving social norms interact to create multiple, divergent logics that will shape future military campaigns. This trend is likely to persist. As societies become more connected, the actors relevant to a given strategy multiply, creating a dizzying array all competing in and through cyberspace. This multifactor competition creates risk of a new anarchy that undermines traditional notions of sovereignty, national security, and deterrence.

In order to develop sustainable nonpartisan strategies, strategic-foresight activities are an essential starting point. These scenarios are only the opening steps of a long journey, suggested paths of discussion and forecasting that chart how growing connectivity will shape the future of strategic interaction and great-power competition. Hopefully, this collection will motivate individuals across government, industry, and civil society to imagine alternative futures against which they can start developing new strategies, organizations, and tactics. For this reason, the authors invite feedback and additional submissions from those who want to expand on the work here, and also welcome those who want to submit their own scenarios to advance the discussion. Growing connectivity alters the character of strategic competition.[18] How people interact creates new spaces and mechanisms for coercing rivals, changing popular sentiment, and undermining political and economic institutions. These three scenarios describe possible futures. Where they point to emerging friction, rapid change, or even seemingly unassailable bureaucratic obstacles, they serve as a warning. Failure to adapt to the changing sociotechnical environment—and the impact these changes have on how people shape understanding, drive collaboration, and decide to act could be crippling.

17 On the competition continuum, see "JDN 1-9 Competition Continuum," Chairman of the Joint Chiefs of Staff, June 3, 2019. On campaigning, see "Joint Concept for Integrated Campaign," Chairman of the Joint Chiefs of Staff, March 16, 2018. On the cyberspace layers, see "JP 3-12 Cyber Operations," Chairman of the Joint Chiefs of Staff, June 8, 2018.

18 Charles Cleveland, et al., *Military Strategy in the 21st Century: People, Connectivity and Competition (New York: Cambria Press, 2018); Parag Khanna Connectography: Mapping the Future of Global Civilization (New York: Random House, 2016); Anne-Marie Slaughter, The Chessboard and the Web: Strategies of Connection in a Networked World (New Haven: Yale University Press, 2017); and Zeev Maoz, Networks of Nations: The Evolution, Structure, and Impact of International Networks, 1816–2001 (New York: Cambridge University Press, 2010).*

# ABOUT THE AUTHORS

**John Watts** is a Senior Fellow at the Atlantic Council's Scowcroft Center for Strategy and Security. Watts has spent more than a dozen years working across the public, private and military sectors in Australia and the US, including as an Army Reserve Officer, Department of Defence policy officer and consultant to US government and military agencies. Over this time his focus has been on Indo-Pacific security; examining the nature of future warfare and the implications of complex emerging security risks. At the Atlantic Council he has continued this work, leading wargames on future conflict; Baltic and Middle East security; in support of developing new military operational concepts and examining emerging military threats; as well as examining Southeast and Austral-Asian security issues. Watts holds a Master of International Law from the Australian National University and a BA in International Studies from the University of Adelaide.

**Benjamin M. Jensen, PhD** holds a dual appointment as a Professor at the Marine Corps University, School of Advanced Warfighting and as a Scholar-in-Residence at American University, School of International Service. He is the author of three books including Forging the Sword: U.S. Army Doctrine, 1975-2010 (Stanford University Press, 2016), Cyber Strategy: The Changing Character of Cyber Power and Coercion (Oxford University Press 2016) and Military Strategy in the 21st Century: People, Connectivity and Competition (Cambria Press, 2018). Dr. Jensen writes a column on the changing character of conflict for War on the Rocks, entitled "Next War." He has received grants and research support from the Carnegie Corporation of New York, Koch Foundation, Office of Naval Research, Hewlett Foundation/University of California-Berkley, the U.S. Marine Corps (Innovation Award), Minerva Initiative, and Smith Richardson Foundation. He is an alumnus of the Philip Merrill Center for Strategic Studies Basin Harbor Workshop, the Bridging the Gap Initiative, the American Academy for Strategic Education, American University School of International Service (PhD 2010, MA 2008), National Intelligence University (MS 2010), and University of Wisconsin-Madison (BA 1997). Dr. Jensen is currently a Non-Resident Senior Fellow at the Atlantic Council and a Senior Research Director with the Cyberspace Solarium Commission. Outside of academia, he is a U.S. Army Reserve officer in 75th Innovation Command.

**JD Work** serves as the Bren Chair for Cyber Conflict and Security at the Marine Corps University, where he leads research to develop the theory, practice, and operational art of the cyber warfighting function, and to explore the wider role of the cyber instrument in national security strategy, and the future defense competition and stability problem space. Mr. Work has over two decades experience working in cyber intelligence and operations roles for the private sector and US government. He previously directed multiple international research programs to provide insight into the emerging strategic issues, economic consequences, and technology implications created by hostilities in the virtual domain. This work has sought to establish a reliable baseline of observations regarding the engagements, follow on effects, capabilities, doctrine, and drivers behind the antagonistic action of potential combatants in the networked environment, in order to support early warning, crisis management and crisis prevention in and through cyberspace. Mr. Work holds additional affiliations with Columbia University's School of International and Public Affairs, Saltzman Institute of War and Peace Studies as well as George Washington University, Elliot School of International Affairs. He further serves as a senior advisor to the US Cyberspace Solarium Commission.

**Nina Kollars** is a non-resident fellow at the Modern War Institute at West Point and an editorial board member for the Special Operations Journal. Dr. Kollars also serves as a Fellow on the Cyber Solarium Commission. Her research interests are on cyber security and military innovation. She has published in numerous magazines and journals to include: "The Rise of Smart Machines: The Unique Peril of Intelligent Software Agents in Defense and Intelligence" in Palgrave Handbook of Security, Risk and Intelligence; "SOFWERX's Return on Collision: Measuring Open Collaborative Innovation" in Special Operations Journal; and "Cyber Beyond Third Offset: A Call for Warfighter-Led Innovation" in War on the Rocks co-written with Jacquelyn Schneider. She holds a PhD in Political Science from The Ohio State University.

**Chris Whyte** is an assistant professor of homeland security and emergency preparedness. His research interests include a range of international security topics related to the use of information technology in war and peace, political communication and cybersecurity doctrine/policy. Dr. Whyte received his doctorate and master's degrees in political science from George Mason University. He was previously a non-resident fellow with Pacific Forum CSIS and a fellow at the Center for Security Policy Studies, George Mason University. Previously, he worked in various roles at several national security think tanks, including the Cato Institute, the Center for the National Interest and the Center for a New American Security.

# Atlantic Council Board of Directors

# Atlantic Council

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.



Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org