

Safeguarding Cyberspace: The Imperative for Reform & Rebalance

Seminar #14 – ES6710 Group Paper

Dr. James R. Van de Velde, Instructor

**The Dwight D. Eisenhower School
for National Security and Resource Strategy
National Defense University**

Executive Summary	2
Framing the Problem.....	2
The Paradox of the Cyberspace Domain.....	6
Evolution of US Cybersecurity Policy	7
Evolution of Social Media as Target of Opportunity	8
Russia.....	10
China	16
The Wide World of Malign Actors.....	21
Recommendations.....	22
Recommendation 1: Appoint a Cyberspace Lead and Establish a Supporting Governance Structure to Shape the Cyberspace Domain	22
Recommendation 2: Cultivate Relationships with the Private Sector to Build Cyber Resilience	25
Recommendation 3: Shape the Federal Government to Take Bold Action	28
Conclusion	29
Annexes	1
Annex A - Acronyms	1

Annex B – Key Cyber Competition Terms.....	3
Annex C – OIE Industry Study Engagement and Speakers.....	5
Annex D – Cyber Employees.....	9
Annex E – Tables and Figures	11
Annex F – Digital Silk Road Addendum Paper	15

The views expressed in this paper are those of the author and do not reflect the official policy or position of the National Defense University, the Department of Defense, or the U.S. Government.

Seminar 14 Student and Faculty Acknowledgment

Author Team

LTC Zoraida Escobar, US Army
 COL Jana K. Fajardo, US Army
 LTC Jessica Goffena, US Army
 COL Erick Komba, Tanzanian Army
 Mrs. Zannia McDonald, Department of the Army
 LTC Mark R. Milhiser, US Army Reserve
 LTC Jessica A. Milloy, US Army
 Lt Col Stephanie Myers, US Air Force
 Mrs. Carla J. Norris, Defense Contract Management Agency
 COL Adel Nurmashev, Kazakh Army
 COL Samuel Preston, US Army

COL Alejandro Rivas Salgado, Mexican Army
 Ms. Sakeena Siddiqi, Department of the Navy
 CDR Brendan Tower, US Navy
 Mrs. Danna Van Brandt, US Department of State
 LTC Altwan Whitfield, US Army

Professors/Instructors

Dr. James Van de Velde, National Defense University (NDU)
 LTC Kevin Harper, US Army
 Mr. L. Reece Smythe, US Department of State

“Cyberspace is a dynamic and inter-connected domain where near-peer adversaries seek to exploit gaps and seams between our organizations and authorities. Such adversaries use a variety of cyber means to compromise our systems, distort narratives and disseminate misinformation. These actions threaten our national interests by impairing the safety and security of our citizens, stealing intellectual property and personal information while seeking to undermine the legitimacy of our institutions.”¹

General Paul M. Nakasone, Commander, US Cyber Command, and Director, National Security Agency, April 2022, in testimony before the Senate Committee on Armed Services

Executive Summary

The United States (US) will most likely continue to suffer unacceptable losses in strategic competition with autocracies in cyberspace until it shapes the cyberspace domain by improving cyberspace attention, leadership, and governance, fostering a more collaborative relationship with private industry to advance digital literacy and cybersecurity, and involving more offensive cyberspace operations through integrated deterrence via defend forward and persistent engagement strategies. Allies and partners should be engaged to ensure synchronous policies. The 2023 *National Cybersecurity Strategy* (NCS), though appropriately advancing cybersecurity, will unlikely bend the positive slope of Intellectual Property (IP) theft, ransomware loss, malign cyber information operations (CIO), and ongoing cyberspace threats to US critical infrastructure by Russia and China. The US remains largely timid in cyberspace, especially in punishing malign actors, fearing escalation to kinetic conflict, and limits itself to cybersecurity. To date, US operations involving denial capabilities have not resulted in escalation to military conflict.

To shape the cyberspace domain to protect US and allied interests and protect US political and economic sovereignty, the United States must:

Figure 1. “Best Friends?”

Source: Heather A. Conley et al., “Countering Russian & Chinese Influence Activities,” www.csis.org, July 1, 2020.

1. Shape the cyberspace domain and out-compete its adversaries, who view their relationships with the US as zero sum.
2. Afford the National Cyber Director (NCD) the authorities to synchronize and integrate US efforts to shape the cyberspace domain, including combating foreign information operations (IO).
3. Invest in emerging technology and public-private partnerships to out-compete adversaries in the cyberspace domain, including expanding cyber resilience, advancing private sector cooperation through a broader cyber incident reporting base, establishing a non-DoD cyberspace Reserve Force, establishing a Federal “Hack Us” program through the Office of the NCD (ONCD) and Cybersecurity and Infrastructure Security Agency (CISA), and enacting bipartisan legislation to protect Americans from malign, foreign cyber information activities.
4. Provide certain Federal government agencies with pre-approved authorities to engage cyberspace threats with proportional, defensive cyberspace operations to deter, disrupt, and destroy malicious cyberspace activity at its source.

Framing the Problem

As the US aims for an open, free, global, interoperable, reliable, and secure internet, autocracies’ gray zone activities in cyberspace sap US wealth and undermine US national interests and democratic values.² The characteristics of cyberspace make it particularly vulnerable to gray zone activities, where adversaries seek changes to the political *status quo* through strategic competition.

Cyberspace is a globally interconnected digital ecosystem that spans the public and private sectors. Cyberspace exists in the information environment, where interrelated layers expand the threat surface with multiple targets and numerous state and nonstate threat actors, including hackers. The US lacks a lead Federal actor with the authority to integrate and synchronize effects in the information environment. There is a distinct division among the Federal cyberspace entities, such as the Department of Defense (DoD), CISA, Federal Bureau of Investigation (FBI), and Central Intelligence Agency (CIA), and their associated authorities. As a result, each of these Federal entities frame the cyberspace domain problem differently, allowing gaps that prevent addressing threats holistically. The US fears escalation often limits its offensive and defensive options, allowing the cyberspace domain to sap US economic and political strength. Knowing this, autocracies, such as China and Russia, aggressively employ gray zone activities as tools of repression and coercion to shape the cyberspace domain to their advantage.³

OIE Takeaway

Most of the US government and industry suffer a sine wave-like pattern of never ending efforts at cyberspace defense, improving defenses but then suffering and discerning new vulnerabilities, and then more defense. endless defense, which shifts from inadequate to excellent like a sine wave over time.

Information Environment

The Information Environment

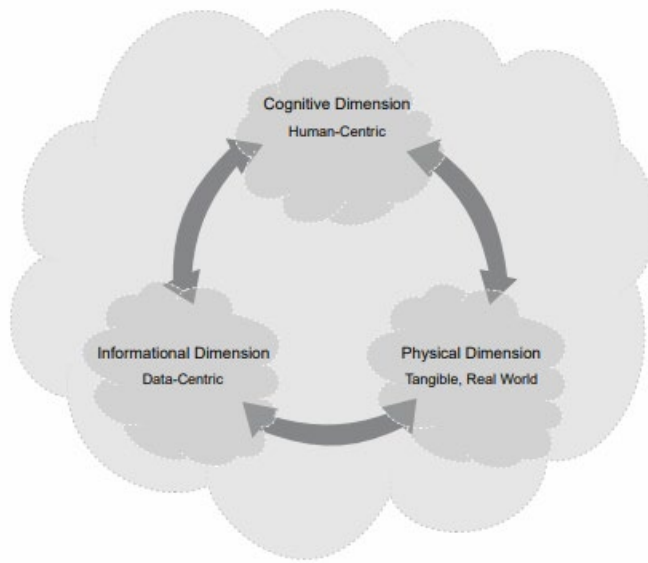


Figure 2. The Information Environment, JP 3-13
Department of Defense Joint Staff, “Joint Publication
3-13, Information Operations, I-2,” November 20,
2014.

The information environment, which includes the cyberspace domain, is difficult to conceptualize. *Joint Publication 3-13, Information Operations*, defines the information environment as “...the aggregate of individuals, organizations, and systems that collect, disseminate, and act on information.”⁴ The information environment comprises three layers: the physical, informational, and cognitive.⁵ States employ and project all instruments of national power in the information environment, including diplomatic, informational, military, economic, financial, intelligence, and law enforcement. (i.e., DIMEFIL).⁶ Operations in the information environment (OIE) include everything from a press release to a cyber-attack. The Institute for the Study of War and the IBM Center for The Business of Government define OIE as “deliberate campaigns to influence others’ wills in which the mechanism of influence is not the

use or threat of violence, but rather nonviolent, non-kinetic methods aimed at shaping others’ perceptions, motivations, and convictions ... [where] human cognition is the key terrain.”⁷ Adversary intent in the information environment ranges from sowing domestic discord, stealing IP, advocating for regime change, provoking political change, shaping opinion, to gathering intelligence. The information environment expands all warfare domains, yet the US does not appoint a lead Federal entity responsible for integrating and synchronizing efforts for the “I” (informational) in DIMEFIL.

Information Environment Layers	
Physical Layer	Command and control systems and associated infrastructure
Informational Layer	Networks and systems where information is stored
Cognitive Layer	The minds of the people who transmit and respond to information.

Figure 3. Information Warfare: Issues for Congress
Catherine A. Theohary, “Information Warfare: Issues for Congress,” March 5, 2018, 5.

Cyberspace Domain

“US military and [North Atlantic Treaty Organization] NATO joint doctrine recognize five domains of warfare: air, sea, land, space, and cyber.”⁸ The cyberspace domain is a warfare domain with three interrelated layers that exist within the information environment, including the physical network layer, the logical network layer, and the cyber-persona layer.⁹ Cyberspace contains data that affect the information environment; cyberspace is not the totality of the information environment.¹⁰ Cyberspace expands all warfare domains, and yet cyberspace also expands the globally interconnected digital ecosystem. The US does not appoint a lead Federal entity responsible for integrating and synchronizing effects within the cyberspace domain. Russia and China are the US’s principal adversaries that leverage OIE, particularly those in the cyberspace domain, to their advantage.

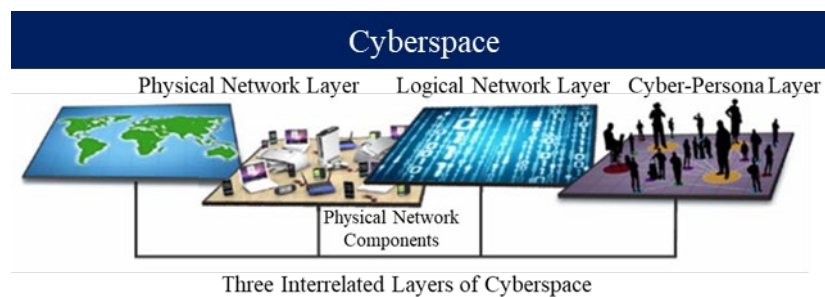


Figure 4. Three Interrelated Layers of Cyberspace

Department of Defense Joint Staff, “Joint Publication 3-12, Cyberspace Operations,” June 8, 2018, Figure I-1, I-3.

Russia’s notoriety related to the use of information in war is probably due to the minimal effort given to disguise its information operations. The Kremlin has paid the price in sanctions, but they have not been an effective deterrent. Meanwhile, China has modernized its approach to information operations in a way that does not attract attention. The Chinese believe the opponent’s perception of facts on the ground is as important as the facts themselves. China is capitalizing on the benefits of the growing imbalance with other states’ attention to information issues. Rob Joyce of the National Security Agency (NSA) described the difference between the two using the analogy of Russia being the hurricane coming in fast & hard. China, on the other hand, is likened to climate change – long, slow, and pervasive.¹¹ However, both are moving along paths to create a perfect storm of content hostility toward the US and its allies.

OIE Takeaway

The US tendency toward *splinterization* is a comparative disadvantage against our adversaries in the competition stage.

The US Suffers a Range of Malicious Cyber Activity and Malign Cyber Information Operations (CIOs)

The US is under constant attack in the cyberspace domain. A recent report noted that the US is a victim of 65 percent of global cyber-attacks.¹² Cyber-attacks zip back and forth across the globe every second in an overwhelming and constant onslaught. See Figure 5 for a one-second snapshot of attacks on May 18, 2023.¹³ The US suffers various malicious cyber activities and malign CIOs with adverse political, societal, and economic outcomes. Malign CIOs (e.g., disinformation and mal-information) erode public trust in democracy by sowing discord, generating confusion, and increasing division in the US.¹⁴ American trust in the government is already low, with only two-in-ten Americans believing the government does what is right.¹⁵ If the US fails to address these threats, it will be increasingly disadvantaged during strategic competition. Threats within the cyberspace domain are not simply a cybersecurity problem. Protecting America's critical infrastructure through defense, deterrence, and negotiation will not effectively shape the cyberspace domain.

Figure 5. Cyberthreat Real-Time Map of attacks taken in a one-second timeframe on May 18, 2023
Source: "MAP | Kaspersky Cyberthreat Real-Time Map."

The Paradox of the Cyberspace Domain

As the Solarium Commission report demonstrates, both Democrat and Republican lawmakers agree that the cyberspace domain needs addressing. Cyberspace – unlike the other domains – is a giant, hot mess. Norms must be defended; political interference by the autocracies must be defeated; threats to US critical infrastructure must be eliminated; economic loss through IP theft and massive espionage data leaks must be blocked. However, successive administrations have approached cyberspace operations as if they are massively dangerous risks to conventional conflict.

There is something about cyberspace that paralyzes strong leadership. Is it because the American people do not see loss and risk in cyberspace, unlike through the other domains, and so action can be avoided without domestic political cost? Or do cyberspace operations still conjure unknown risks to leadership, and thus leadership avoids action? Nevertheless, inaction is accepting risk too – the most certain fact is that subsequent malign activity will continue since the autocracies currently do not seem to fear unacceptable punishment through cyberspace.

Adding to this paradox is the historical fact that military cyberspace operations carry the least risk of escalation of all warfare domains. Cyberspace operations have yet to escalate to kinetic violence. Yet, successive administrations have labored intensely to review, slow, and limit their conduct.

Puzzling is that a US O-6 in Iraq can independently order military strikes against high-value ISIS individuals based on (area of hostilities) command authorities, but in many cases changing a zero to a one on a website somewhere in the world (to deny its function) requires Presidential approval. Of course, there are legitimate concerns over such cyberspace activities – many of which involve

violations of sovereignty. However, the cyberspace domain is the least defended yet the most complicated by interagency concerns and fears of escalation.

Evolution of US Cybersecurity Policy

The Bush Administration published the first *National Strategy to Secure Cyberspace* in 2003. It established a framework to minimize cyber vulnerabilities¹⁶ to protect the “nervous system of US critical infrastructure.”¹⁷ Key actors for threat reduction at that time included the FBI, the

OIE Takeaway

A 'whole of government,' integrated approach is needed to counter malign cyberspace actors and foreign disinformation campaigns.

US Secret Service, law enforcement, and parts of the nascent Department of Homeland Security (DHS).¹⁸ The Department of State (DoS) was charged to promote and develop an international coalition mission cooperation,¹⁹ and the private sector was encouraged to develop standardized IT certifications for professionals.²⁰ While the US retained the right to conduct offensive cyber operations (OCOs) against any adversary if required, there is little evidence that any OCOs took place.

President Obama strengthened cyber defenses and facilitated cyber threat warnings across the Federal government,²¹ but also struggled with using offensive cyber capabilities. To strengthen the US defensive cyber posture, US Cyber Command (USCYBERCOM) became a combatant command for the cyberspace domain in 2010.²² It focused on defending the DoD Information Network, supporting other combatant commands, and strengthening the US capacity for withstanding and responding to cyber-attacks.²³ Soon after, DoD published its first cyber strategy in 2011 that focused on defense, deterrence, and building relationships but lacked discussion of offensive actions or capabilities.²⁴

In 2013, Edward Snowden leaked classified government materials, which included Obama's Presidential Policy Directive 20 (PPD-20).²⁵ The document recognized the valuable range of offensive cyber options below the threshold of war but cautioned against the unintended consequences and collateral risks of using them.²⁶ As a result of the document's illegal public disclosure, President Obama published an unclassified process to launch OCOs that implemented a cumbersome process that required multiple levels of approval, up to the President, practically discouraging any use at all.²⁷

Figure 6. US Cyber Command Activated

Source: “Gates establishes US Cyber Command, names first commander,” Air Force News, (May 21, 2010).

The Obama administration subsequently maintained a defensive posture but was more transparent with its cyber strategy, publishing a 2015 update.²⁸ This update identified malicious actors such as China for IP property theft and outlined the cyber capabilities of Russia, but reinforced a policy of restraint as it created a DoD element naturally postured for countering such activities.²⁹ Obama also passed the *Cybersecurity Act of 2015*, which encouraged public and private sector cybersecurity information sharing through CISA but made engagement with CISA optional.³⁰

The Trump administration changed the posture for US cybersecurity in 2018, flattening the Obama-era approval process for OCOs and reevaluating their risk, two hallmarks of Obama's

PPD-20 and his subsequent unclassified document.³¹ This change was "intended to help support military operations, deter foreign election influence, and thwart IP theft by meeting such threats with more forceful responses."³²

Following the reversal of President Obama's policy, the Trump administration published its *National Cyber Strategy* in 2018,³³ which included a higher tolerance for risk, less concern about escalation, and allowance for deterrence and punishment to preserve peace.³⁴ The companion *DoD Cyber Strategy* outlined a new defensive concept called 'defend forward,'³⁵ a daily, ongoing homeland defense mission that directs DoD to work with the private sector³⁶ and attempts to stop threats outside the US before they reach US targets such as critical infrastructure.³⁷ This was a monumental shift and identified the vulnerabilities existing in public-private relationships, thereby necessitating partnerships and defense for the private sector.

The Biden administration published its cyber strategy in 2023. It predictably took an approach closer to the Obama administration, advocating for a return to a defensive posture with a resilient and robust defense. However, regarding offensive operations, the strategy offers only "minimally invasive actions."³⁸ As the DoD and USCYBERCOM develop their own cyber strategy to nest with the NCS, the DoD must determine how USCYBERCOM will integrate cyberspace operations to defend against malicious actors threatening US interests.

Figure 7. Defending forward

Source: Robert Chesney, "The 2018 DoD Cyber Strategy," Lawfare, (September 25, 2018).

Evolution of Social Media as Target of Opportunity

Although social media provides its users with positive benefits, its popularity and connectedness serve as vulnerabilities that provide malicious actors with far-reaching access. Social media use exploded in the twenty-first century, allowing worldwide instant communication. Friendster, founded in 2002, was the first social media site to establish a global presence, followed shortly by MySpace.³⁹ Facebook emerged in 2004, took control of the market, and continues its dominance today. Twitter introduced a different business model focused on micro-blogging in 2006. Other platforms continue to break into the social media sector to establish a foothold and fight for market share.⁴⁰ Activists and ordinary people use social media platforms to share stories, engage in discussion, and make their voices heard. Therefore, it is unsurprising that society has used social media to organize and coordinate social movements worldwide, such as the Arab Spring from 2010 to 2012.⁴¹

Figure 8. Social Media Across the Globe

Source: Colm Russell, "Social Media Recruitment – Driving Change for International Data Collection," Dynamic Fieldwork, accessed May 11, 2023.

Foreign actors readily connect with millions of Americans in cyberspace to influence beliefs, attitudes, behaviors, and decisions. According to current 2023 estimates, over 308 million Americans are on social media, roughly 90 percent of the population. By 2028, as seen in Figure 9, projections are that there will be over 331 million.⁴² Research indicates rumors and false information diffuse across social media further, quicker, deeper, and broader than accurate information.⁴³ Social media amplifies messages using algorithms that prioritize, recommend, and disseminate information that users prefer – typically content that confirms what the user already believes without regard for accuracy.⁴⁴

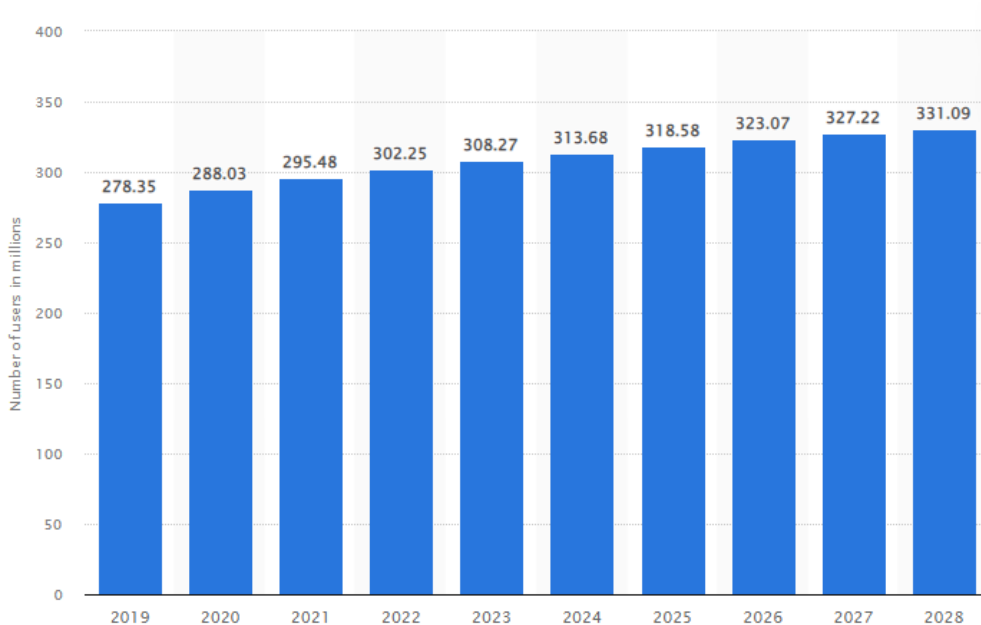


Figure 9. Number of Social Media Users in the US from 2019 to 2028 (in millions)

It is easier to hide in plain sight with techniques like information laundering that obscure the originator's identity while influencing perceptions, gaining followers, and normalizing positions.⁴⁵ The internet ecosystem enables fake news to spread across entire networks. Information can now cross platforms and reach millions of people instantly—significantly more than traditional media sources like print newspapers or radio broadcasts.⁴⁶ In 2013, a Twitter account posted a bogus tweet claiming two explosions had injured President Obama at the White House.⁴⁷ The tweet reached Wall Street and, in less than two minutes, caused a collapse of almost 143 points and a loss of over \$136.5 billion.⁴⁸ Additionally, a war's fate is no longer determined solely by bullets and bombs but includes effects from the weaponization of the internet and social media can impact the outcome of war.

Social Media Bot Army

Bots, software programs that complete repetitive tasks quickly in networks, are essential for the general running and maintenance of the internet and especially important for the functioning of search engines.⁴⁹ However, the evolution of bots and the introduction of artificial intelligence (AI) technology yielded social media bots, which are programs that communicate over multiple social media pathways, including voice, text-based chat, and video.⁵⁰ Social media bots can display human conversational behaviors and appear legitimate, adding credence to their assertions online; unfortunately, most of these bots are considered malicious and, depending on the source, comprise 5-15 percent of social media accounts.⁵¹

The influence of social media bots represents an invisible hand in American politics and social discourse. During the 2016 US presidential election, social media bots accounted for 20 percent of political communication in the days before the election.⁵²

The potency of social media bot-enabled information operations will increase with evolving technology. Snapchat recently fielded a new AI chatbot, *ChatGPT*, a capability providing an AI persona, complete with an avatar, voice, and text chat functions.⁵³ Society is moving from individuals having a transactional relationship with technology toward people having conventional interpersonal relationships with tech entities.⁵⁴ The US government (USG) and national security strategists are not prepared for this change. If they are not already, advanced AI using deep fake personas, voices, and text will soon enter established partisan social media echo chambers to influence political and social discourse. AI-powered social media bots masquerading as public figures and American citizens are a potential threat to national security, the responsibility for which is shared between the public and private sectors. The influence of social media bots will increase technological advances, including in the public square of democracy.

Russia

Figure 10. Social bots

Source: Nick Bilton, "Social media bots offer phony friends and real profit," The New York Times, (November 19, 2014).

"The aim is not to make you love Putin. The aim is to make you

disbelieve anything. A disbelieving, fragile, unconscious audience is much easier to manipulate."

E.U. Official⁵⁵

Russia Malign Information Operations

Russian information warfare strategy to disrupt other countries includes "weakening and undermining societies...to influence policies of another government, undermine confidence in leaders and institutions, disrupt relations between other [states], and discredit political opponents...and to conquer the mind and soul of the people."⁵⁶

In the early 2000s, Russia invested in cyber capabilities to repress domestic opposition groups and independent media.⁵⁷ Since then, its cyber capability has morphed into a crucial tool of foreign

policy used by multiple Russian government agencies – the Foreign Intelligence Service (SVR), the Federal Security Service (FSB), the Federal Protective Service (FSO), and the Internet Research Agency (IRA). By design, no single agency is responsible for cyber operations, making attribution harder for the US and the international community.⁵⁸ The topics vary. However, the narrative is the same, “don't trust anyone.”⁵⁹ The Kremlin weaponizes information, culture, and money⁶⁰ to manipulate opinion and decision-making.⁶¹ It exploits societal fractures or seeks to divide a populace to undermine democracy. Whereas the former Soviet Union backed a unified anti-US policy message, the Kremlin does not push a specific agenda. Instead, it exploits issues by posting on far-left or far-right-wing websites to widen the divide between the US and allied countries. It uses social media as a weapon to erode the integrity of investigative and political journalism.⁶²

OIE Takeaway

The Internet has proven to be a tool in promoting democracy, but authoritarian governments harness the Internet's power to serve their purposes as well: surveillance; propaganda; monitoring; herding.

Perhaps most critically, the Kremlin executes these operations below the level of armed conflict, taking advantage of the lack of agreed-upon international customs and norms. There are disputes as to what constitutes a violation of sovereignty, a very high bar of what constitutes an “attack,” and even more complex are the requirements needed to officially “attribute” activities to a malign actor.⁶³ These gray zone activities, “coercive approaches that may fall below perceived thresholds for US military action and across areas of responsibility of different parts of the [USG],”⁶⁴ paralyze the West’s response.

What is the Kremlin’s purpose?

The Kremlin designs its IO to destroy faith in democratic institutions – the US government, democratic processes, and the media. Its goal is to create chaos in US society and sow confusion among US citizens.⁶⁵ It is to “prevent reform at home and weaken opponents abroad.”⁶⁶ Putin demonizes liberal democracies as prurient, expansionary, shallow, and threatening to the Russian nation to preserve internal control and galvanize his people, and laments the dissolution of the Soviet Union.⁶⁷ He has used IO to weaken the West, particularly the United States, with messaging designed to foment internal division.⁶⁸ To achieve these end states with the limited resources available, the Kremlin uses IO because it is cheap, effective, and it allows the Kremlin to maintain plausible deniability avoiding the risks of kinetic retribution.⁶⁹

General Paul M. Nakasone, Commander, USCYBERCOM, stated in an address to the 118th Congress Senate Committee on Armed Services on March 7, 2023, “Foreign attempts to meddle in our electoral process via cyber means escalated in 2016 and have persisted in every election cycle since.”⁷⁰ The USCYBERCOM anticipates this behavior continuing to not only divert leadership but to drive a wedge between Americans in general while “undermining public trust in the democratic process.”⁷¹

Figure 11. General Nakasone

Source: Amy McCullough, “Ukraine Crisis to Influence Growth of US Cyber Force, Nakasone Says,” Air & Space Forces Magazine, April 6, 2022.

As General Nakasone stated, this behavior is cost-effective and will probably continue. However, it bears noting that some of the literature reviewed, including an article in the *National Review* in February 2023, cited studies indicating Russia's meddling had minimal effect on the 2016 election. The article intended to paint a cautionary tale about potential governmental censorship as a justification to protect democracy's health.⁷² Others indicate the Russians "did nothing more than mimic American-born political sentiments," which were already being captured by many US voices.⁷³ Nonetheless, having a greater understanding of Russian malign activities must inform US strategies in the future.

OIE Takeaway

The authoritarian states exploit the information environment to advance the decline – even collapse – of the US and liberal democratic states.

United States Presidential Election: 2016

Pursuant to Russia's methods of cyber intrusion into US society, Russia has not advocated for a particular candidate – Russia only seeks to disrupt democratic processes. "The IRA's method of inducing trust and believability that lead to 'spreadability' is what they used going into the 2016 US election."⁷⁴ Russian trolls exploited the existing sentiment against candidate Hillary Clinton that stretches back to the 1990s and the Whitewater controversy. Using this base of existing believers, Russia amplified negative messages around issues like stolen John Podesta (Clinton's campaign manager) emails, Clinton's private server misuse during her time as Secretary of State, and alleged Democratic National Committee (DNC) corruption. The US identified two units within the SVR (formerly GRU) responsible for hacking the DNC.⁷⁵

Russia amplified its chosen messages via social media bots. Estimates indicate Russia used between 16,000 and 34,000 Twitter bot accounts that reportedly reached 1.4 million users.⁷⁶ At the Oxford Internet Institute, the Computational Propaganda Research Project discovered that in 16 swing states, "seven million tweets used hashtags related to the 2016 election" within the first two weeks of November 2016.⁷⁷ False Facebook IRA accounts "exposed 126 million users to political disinformation" before the 2016 election.⁷⁸ In 2016, a *New York Times* reporter, Adrien Chen, interviewed those in the troll network. They stated that their purpose in the 2016 election process "was not to brainwash readers, but to overwhelm social media with a flood of fake content, seeding doubt and paranoia, and destroying the possibility of using the Internet as a democratic space."⁷⁹ Trump lost the popular vote by 2.8 million votes but won the electoral by only about

80,000 votes.⁸⁰ Figure 12 demonstrates the magnitude of social media reach in the 2016 election.

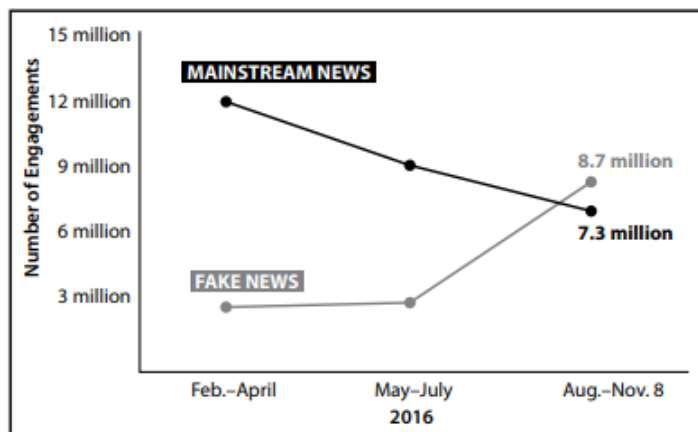


Figure 12. Total Facebook engagements for the top 20 election stories
Source: Lt Col Jarred Prier, "Commanding the Trend: Social Media as Information Warfare," *Strategic Studies Quarterly* Vol. 11, no. 4 (Winter 2017): 61.

United States Presidential Election: 2020

Russia used similar tactics during the 2020 US presidential election, but its chosen rhetoric centered on magnifying the voter fraud story. Intelligence supports that China and Iran also targeted the US, all three seeking to advance social unrest and distract the US public toward domestic issues (and away from foreign policy).⁸¹ As noted above, studies show that most social media users are more likely to share a false story than an accurate one, and this is especially true for political news. A Brown University study from 2020 indicated that false tweets on Twitter had a 70 percent better chance of being retweeted. A comparable Edelson Study in 2021 revealed that fraudulent Facebook posts attracted six times more viewers.⁸² There is no empirical data to support that sharing false information implies it is believed; however, a “fundamental principle of human social networks is that they magnify whatever they are seeded with,” according to Nicholas Christakis, director of the Yale University Human Nature Lab.⁸³ This seeding, whether a false narrative or not, creates media bubbles that isolate voters from opposing views through algorithms.⁸⁴

United States Midterm Elections: 2022

By the time the 2022 US midterm elections were underway, the USG had created whole-of-government mechanisms to better counter Russian disinformation efforts to taint the democratic process. The intelligence community and law enforcement worked collectively, including USCYBERCOM, the NSA, DHS, and the FBI. The Election Security Group (ESG), staffed by USCYBERCOM and NSA, served as a central coordination hub for operations, intelligence, and cybersecurity. As a result, there was reportedly minor successful “foreign malign influence or interference” in the primaries or certification process.⁸⁵ CISA and USCYBERCOM’s National Mission Force (CNMF) played an instrumental role in the midterm election success.⁸⁶ “CISA proactively identified potential intrusions ... [and fed] actionable information” to the CNMF for defend forward type operations to combat the threat.⁸⁷

Ukraine Presidential Election: 2019

As in the case of Russia’s meddling in the 2016 US presidential elections, the Russian intent in Ukraine was to discredit “the [Ukrainian 2019] election process [and undermine] Ukrainian authorities.”⁸⁸ Russian propaganda centered on claims that the 2019 Ukrainian elections were unlawful and falsified and that the results should not be trusted regardless of the outcome. While Russian efforts did not appear to favor one candidate over the other, it did result in an underwhelming 61 percent voter turnout, indicative of “a general disenchantment with democracy on the part of the Ukrainian electorate.”⁸⁹ While Russia has historically used disinformation and

OIE Takeaway

Influence campaigns are more likely to be accepted if backed by alleged 'evidence,' even if that evidence is false.

propaganda, its reach has grown tremendously, given the explosion of social media and increased use and accessibility of the Internet. As of November 2022, Ukrainian internet usage was 75 percent, and 89 percent of Ukrainians have “at least 3G mobile technology.”⁹⁰

Assessing the Effectiveness of Russian Malign Influence Operations

“Russia’s carefully orchestrated, sophisticatedly targeted, generously funded, and professionally produced disinformation campaign has met little effective resistance.”

INFOWAR Papers⁹¹

The IRA’s expansive reach during the 2016 US Presidential election illuminates the Kremlin’s effectiveness, and it was amplified again during the Black Lives Matter movement, in which the IRA released thousands of divisive advertisements targeting both sides. An estimated 3.7 million users clicked on the IRA advertisements on Facebook.⁹²

The discussion of the Kremlin’s attempts to disrupt US democratic processes generally focuses on whether Russian influence changed election outcomes. However, the real story – the real success – from the Kremlin’s vantage point is the vicious infighting that ensued in these events, even if it did not result in a political change. Many international examples have shown that the Kremlin’s IO likely “incites and exploits the protest potential of the population.”⁹³ Their subtle influence is no less compelling. Figure 13 represents the five pillars built in Russia’s malign IO ecosystem.⁹⁴

There are weaknesses in Russia’s information warfare, too, primarily that it is repetitive and predictable.⁹⁵ But, even with predictable content, enough fault lines (i.e., divisive politics) exist in US society to create accessible opportunities for exploitation. In other words, the US is a soft target. “Efforts at social manipulation are effective to the degree that vulnerabilities in a society allow them to be effective.”⁹⁶ Even if Putin has lost credibility among Americans due to the war in Ukraine, a typical lack of attribution online means this diminished credibility is unlikely to hamper the effects of the Kremlin’s influence operations. This period is considered a post-great power competition. Russia’s willingness to be fluid and flexible in supporting any narrative (even if it goes against Russian values or beliefs) to sow discord boosts its remaining effectiveness.⁹⁷

OIE Takeaway

The Law of Armed Conflict applies in cyberspace but what constitutes Defensive Cyber operations, Response Options, needs to be better understood among allies.

Russian Attacks in the Cyberspace Domain

Russia preys on US and global citizens in the information space to build its national power and compromise the security of other states. According to the 2020 *Report of the Cyberspace Solarium Commission for Defense against Cyberattacks*, cyber deterrence efforts have failed to prevent Russia’s malign cyber operations.⁹⁸ In 2007, Russia directed a 22-day cyberattack on the Estonian President, government, parliament, police, banks, internet service providers, online media, many

Figure 13. Russian Disinformation Modus Operandi

small businesses, and local government sites.⁹⁹

In 2017, Russia launched the NotPetya cyberattack, noted as the most destructive cyberattack to date.¹⁰⁰ While the attack was meant to compromise Ukrainian financial networks through tax and

accounting software programs and disguise itself as ransomware, the tolls were much higher and widespread. The malware did more than \$10 billion of damage, disrupting email systems, file access, and logistics while wreaking havoc for multinational companies much further than Ukraine.¹⁰¹

Just a year ago, when it invaded Ukraine, Russia coupled cyberattacks with disinformation, attacking Ukrainian banks and automated teller machines and simultaneously sending texts to Ukrainians to tell them they could not withdraw money.¹⁰²

Russia uses an integrated approach in its attacks. A March 2023 leak to Western media outlets revealed the extent of Russian private-sector collaboration. Moscow-based cyber firm Vulkan contracted with the GRU's Sandworm organization and orchestrated cyberattacks on critical infrastructure and disinformation attacks to undermine US elections.¹⁰³ The leak revealed sophistication, innovation, and a strategy synchronizing cyberattacks and IO.¹⁰⁴

Most recently, in May 2023, the US Department of Justice (DoJ) announced it disrupted a decades-long Russian cyber espionage campaign that stole sensitive information from computer networks in dozens of countries, including the US and other NATO members.¹⁰⁵ The operation accused the Russian FSB of using Snake malware to steal documents, noting it was the most sophisticated malware they had seen from the Russian government over the decade of their investigation.

Assessing Effectiveness of Russian Cyber

Russia is primarily considered the world leader in offensive cyber capabilities and has demonstrated a willingness to use those capabilities, although not without shortcomings. Regarding talent, Russia has actively recruited cyber experts since the 1990s, aligned their educational institutions to be cyber talent pipelines, hired cyber criminals into state agencies, and created capture-the-flag type cyber competitions at schools and universities nationwide as a recruiting mechanism as early as 2010.¹⁰⁶

The 2007 cyberattack on Estonia demonstrated the Kremlin's effectiveness at targeting, although the global losses spanned well past their intended target. The recent newsbreak of the 20-year Russian cyber espionage operation and the amount of time it took the US DoJ to shut it down indicates how sophisticated Russia's operations are in cyberspace. Time and again, Russia proves it has the technical capability and propensity for using cyber as a means of offensive damage and targeting cyber-connected assets. While technical expertise is there, they have significant issues in this realm that can stifle their effectiveness in the future.

OIE Takeaway

Information operations are used by Russia to confuse the target and by China to re-direct the target (by changing the subject); they are not used to persuade recipients of the righteousness of their regimes.

The Kremlin lacks a cyber command. A centralized organization focused on operations in the cyber realm would provide unity of effort to maximize effects and deconflict friendly agencies. However, as previously stated, the decentralized approach complicates attribution, giving Russia the plausible deniability, it prefers. The US established USCYBERCOM to improve the unity of

effort in 2010. Although Russia has numerous cyber agencies in the public and private sectors to call on for cyber operations, the Kremlin does not provide a clear delineation of “operational responsibility and no uniform system of reporting and accountability.”¹⁰⁷ This could explain why Russia’s cyber efforts against Ukraine were so lackluster in the February 2022 invasion – its leadership focused on the more “conventional” part of its “special military operation” with no centralized cyber lead. Russia has the potential to maximize its capabilities if it restructured its cyber efforts.

Figure 14. FBI Wanted Posted for Six Russian GRU Hackers

Source: Andrei Soldatov and Irina Borogan, “Russian Cyberwarfare: Unpacking the Kremlin’s Capabilities,” CEPA, September 8, 2022.

China

China’s use of cyber influence beyond its borders has less history when compared to the depth of Russia’s but matches in sophistication. The Chinese Communist Party (CCP) has gained near total control of Chinese-language media in the US, ensuring Chinese-speaking Americans receive CCP-approved information.¹⁰⁸ The CCP employs a “keyboard army” to promote policies, harass critics, and monitor global discourse.¹⁰⁹ Some Chinese operatives are now under investigation by the FBI for attempting to influence US local politicians.¹¹⁰ China also censors critical content in the United States. A study of CCP influence in Hollywood found it so pervasive that film executives “think about whether something is going to be perceived as criticism, [they] worry about inadvertently crossing some line,” self-censoring to avoid any accidental missteps that may cost them the Chinese audience.¹¹¹ The CCP has long employed data collection to control its population. It now seems to be gathering data on US populations. Leveraging individual global data is new terrain for influence warfare, and China is at the forefront. US officials have identified CCP operatives responsible for massive data hacks and have speculated that this could improve the CCP’s ability to attract intelligence assets. Still, trends suggest that the CCP’s ambitions go beyond recruiting spies.¹¹²

China Malign Information Operations

The Chinese government views the internet as a tool for social control and has invested heavily in building its cyber capabilities. In the early 2000s, when the internet was still in its infancy in China, the government implemented the “great firewall,” a system designed to monitor and censor online

Figure 15. Chinese Soldiers Conducting Information Review and Operations

Source: Remco Zwetsloot, “The US needs multilateral initiatives to counter Chinese tech transfer,” Tech Stream, (June 11, 2020).

activities.¹¹³ This system remains in place, making it challenging for foreign companies and organizations to operate in China.

Figure 16. China's Firewall

Source: Shira Ovide, “Copying China’s Online Blockade,” The New York Times, (March 1, 2021).

The Chinese government also established the “Golden Shield

Project,” a national surveillance and censorship system that aims to monitor and control the online flow of information.¹¹⁴ This project employs a state-sponsored hacking group, which has become China’s new weapon of choice.

A prominent Chinese hacking group from the southwestern Chinese province of Sichuan is APT41. The group is unique in engaging in cyber espionage and financial theft, including the theft of at least \$20 million in US COVID relief benefits.¹¹⁵ APT41 has been linked to attacks targeting the gaming industry, healthcare sector, and telecommunications companies in at least 14 countries.¹¹⁶ China has also pursued a “cyber sovereignty” policy to establish laws and regulations for its corner of cyberspace. Many countries and organizations have criticized this policy as it could further fragment or splinter the internet and limit freedom of expression online.

China Social Media Information Operations

China’s history with IO in social media tracks a progression in narratives, audiences, and approaches. China’s 2011 *Military Dictionary* described public opinion warfare as “creating a favorable public opinion environment for political initiative and military victory” through the “comprehensive use of various media means and information resources to fight the enemy.”¹¹⁷ From their perspective, the US’s extensive engagement in internet infrastructure, service providers, and de facto use of the English language constitutes a threat in public opinion warfare which justifies defensive actions.¹¹⁸ Public opinion warfare continues in times of both peace and war, with peacetime operations aimed at “long-term infiltration into the objects of the society’s and culture’s deep structure, changing the awareness and conviction of the enemy masses.”¹¹⁹

The People’s Liberation Army (PLA) is one of the many Chinese government agencies engaged in IO, including propaganda efforts.¹²⁰ PLA social media experts train in political warfare to improve the PLA’s image and correct misperceptions.¹²¹ China operates its propaganda campaign through the *United Front*, a government agency primarily focused on diaspora relations.¹²²

OIE Takeaway

Chinese Information Operations are more sophisticated - either pulling you in or changing your thinking.

The United Front demonstrates the shift in the Chinese narrative and its IO that expanded from promoting the “China Story” to tackling US concerns in the first half of 2020.¹²³ Marking the shift in audience, BuzzFeed News reported in March 2019 on the first indications of Chinese persona accounts or trolls on Western social media.¹²⁴ Actual attribution occurred in August 2019, when Twitter removed China’s state-sponsored tweets regarding the Hong Kong protests.¹²⁵ Significantly, these tweets proved that Chinese social media IO were aimed at Western audiences for the first time.¹²⁶ They also indicated China’s study of Russian and Iranian techniques: “using high-volume bot accounts, co-opting spam infrastructure (Twitter clients) to spread political messages, and amplifying controversial content.”¹²⁷

In March 2020, China exploited a combination of falsely generated accounts and repurposed

China's Toolbox for Global Media Influence



www.freedomhouse.org

Figure 17. How China Influences the Globe

Source: Sarah Cook, "Beijing's Global Megaphone," Freedom House, (2020).

accounts, indicating coordinated, systematic postings to alter international COVID messaging and deflect criticism.¹²⁸ Similarly, in June 2021, ProPublica and the *New York Times* reported on Uyghur content videos attempting to directly rebut and discredit Secretary of State Mike Pompeo's anti-CCP speech.¹²⁹ The report proved that China generated counterfeit content in direct response to Western reports.

Chinese Threat Activity in the Cyberspace Domain

The capacity and capability of US adversaries in cyberspace exceeds the US in the former and rapidly approaches equivalency in the latter as described in the 2023 NCS.¹³⁰

"The People's Republic of China (PRC) now presents the broadest, most active, and most persistent threat to both government and private sector networks and is the only country with both the intent to reshape the international order and, increasingly, the economic, diplomatic, military, and technological power to do so. Over the last ten years, it has expanded cyber operations beyond intellectual property theft to become our most advanced strategic competitor with the capacity to threaten U.S. interests and dominate emerging technologies critical to global development."

In his article “What China Wants from Cyberspace,” author Adam Segal suggests that China has an ambitious cyber strategy that includes defensive and offensive elements. The country’s goals include improving its economic competitiveness, maintaining political stability, and strengthening its military power.¹³¹ China’s cyber strategy aims to regulate and control cyberspace, advance domestic technology, and develop offensive cyber capabilities to accomplish these objectives.¹³² China has consistently engaged in OCO for the past two decades. These operations target critical military and civilian nodes such as command and control servers and logistics networks. The country’s leaders have consistently worked to become a “cyber superpower.” These operations aim to deter or disrupt adversary intervention and retain the option to scale these attacks to achieve desired conditions with minimal strategic cost.¹³³

According to a Council on Foreign Relations article, “China has set ambitious goals to become a cyber power with an advanced centralized and integrated cybersecurity regulatory regime that will govern data and information flows domestically and globally.”¹³⁴ A report by the NATO Cooperative Cyber Defence Centre of Excellence states, “China’s cyber strategy is about controlling information and data flow on the internet, supporting economic development, and enhancing its position on the global stage.”¹³⁵

OIE Takeaway

We tend to think about the conflict between democracy and dictatorship as a conflict between two different ethical systems, but it may be a conflict between two different data-processing systems.

China’s OCO has caused economic damage in multiple countries and has disrupted the global economic landscape. To bolster its resources, China even stole from American citizens. In 2020, FBI Director Christopher Wray declared, “[It is] the people of the United States who are the victims of what amounts to Chinese theft on a scale so massive that it represents one of the largest transfers of wealth in human history.”¹³⁶ He continued highlighting China’s theft of personal information from 150 million Americans from Equifax, 21 million employment records from the Office of Personnel Management, and the personal data of 80 million Anthem Health Insurance clients. The People’s Republic of China (PRC) also hired criminal contract hackers to steal patented and proprietary information from American firms, increasing their resources at a cost to US prosperity and security. The

FBI estimates China’s unlawful theft cost the US economy between \$225 and \$600 billion annually.¹³⁷

While official statements by the Chinese government suggest that the country adheres to a “defensive” cyber strategy, evidence indicates China is increasingly engaged in OCO to improve its military landscape.¹³⁸ China views its national security challenge as mainly non-traditional, including threats like terrorism, cyberattacks, and regional conflict.¹³⁹ Therefore, China has strategically emphasized the importance of network operations, space-based assets, and cyber capabilities to enhance national security. Two specific ways China has used malign OCO to enhance its military are 1) to sponsor state hacker groups to steal and 2) to transform stolen IP into

Figure 18. FBI Director Address on China Cyber Threat
Source – Christopher Wray, “The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States,” FBI News, (July 7, 2020).

a mechanism to modernize military assets. Figure 19 lists China’s military equipment modernized using stolen IP.¹⁴⁰

	Original design	Chinese version
 Air superiority fighter	Lockheed Martin F-22 (USA)	Chengdu J-20
 Stealth multi-role aircraft	Lockheed Martin F-35 (USA)	Shenyang J-31
 Multi-role combat aircraft	Lockheed Martin F-16 (USA)	Chengdu J-10
 Unmanned combat aerial vehicle	General Atomics MQ-9 Reaper (USA)	CASC Caihong-4
 Transport aircraft	Antonov AN-12 (Russia)	Shaanxi Y-9
 Advanced jet trainer	Yakovlev Yak-130(Russia)	Hongdu L-15
 Armoured car	General HMMWV "Humvee" (USA)	Dongfeng EQ2050

Other key weapon systems reportedly leaked

- Terminal High Altitude Area Defense-Anti-ballistic missile defense system.
- V22 "Osprey" – Tiltrotor military aircraft
- UH-60 Black Hawk-Utility helicopter
- Warfighter Information Network-Tactical(WIN-T) – US Army tactical wireless network backbone for field communication
- Littoral Combat Ship – Surface vessels for near-shore operations

Figure 19. Chinese Military equipment modernized using IP

In 2015, China established a modern and sophisticated military unit, the Strategic Support Force (SSF), to ensure the seamless integration of advanced technology and modern warfare in the Chinese military.¹⁴¹ The unit provides information support for military operations. The SSF's role has become more prominent in recent years, specifically in defending against cyberattacks and maintaining the security of Chinese military information systems. Developments by the SSF have led to several high-profile incidents carried out by Chinese military hackers.

China Offensive Cyber Operations

OCO, including cyber-enabled IP theft, have allowed China to develop and test new military technologies and capabilities more quickly than the US and at a lower cost. In 2014, the US DoJ accused five Chinese military hackers of stealing trade secrets from several US companies in the energy and defense sectors. The indictment spurred a change in US policy toward China's cyber operations.¹⁴² It was the first time members of China's military were formally charged with cyber espionage. Figure 20 provides a visual depiction of China's Cyber espionage activities since 2006.¹⁴³

Figure 20. China's Cyberespionage activities since 2006

It is difficult to determine the financial cost of cybercrime to the US public and private sectors based on the undiscoverable and non-attributable design of Chinese cyber espionage. However, according to a report by the US-China Economic and Security Review Commission, Chinese cyber espionage against the US has been ongoing for approximately two decades, with a significant increase in frequency and scope and few charges brought against attackers.¹⁴⁴ China successfully camouflages OCO to achieve its national security goals. Through cyber espionage, China has been

able to steal sensitive military and defense-related information from the US and international communities.

China's operations hinge on "establishing the country as a global hegemon in the international order and on the key objective of maintaining positive global opinion."¹⁴⁵ The efforts to develop and maintain a positive global reputation have been curated through an international media empire with state media bureaus, foreign media companies, and overseas partnerships.¹⁴⁶ Chinese officials contract for radio broadcasts, work through diplomats, submit op-eds to influential publications, conduct interviews with US media outlets, and pay for *China Daily* inserts in publications like the *Washington Post* and *New York Times*.¹⁴⁷

OIE Takeaway

"We have been in an information war since we gained independence. There is no permanent victory in an information space." – *Estonian MoD Official*

The Wide World of Malign Actors

Countering malign activities and OCO from Russia and China occupies most of the social media bandwidth and attention from the US private and public sectors, but other actors also require attention. Iran, North Korea, and non-state actors share a crucial advantage: they are subject to such heavy international sanctions that they are virtually immune from cyber laws and norms; they have nothing to lose. This immunity, combined with their ability to access illicit markets, has given rise to proxy cyberattacks.¹⁴⁸ These actors also possess outsized cyber capacity, presenting an almost inevitable future of IO for hire. The 2018 estimates suggest North Korea employs approximately 7,000 workers promoting policies and ideology to South Korean audiences.¹⁴⁹ Iran has used IO to promote pro-Iran narratives and counter US influence in the Middle East.¹⁵⁰ While these operations have had regional targets so far, it is feasible that these actors leverage cyber capabilities to conduct IO for hire elsewhere, opening up a new threat environment that would involve actors driven not only by anti-US ideology but with pure financial motivations as well.

"The governments of China, Russia, Iran, North Korea, and other autocratic states with revisionist intent are aggressively using advanced cyber capabilities to pursue objectives that run counter to our interests and broadly accepted international norms. Their reckless disregard for the rule of law and human rights in cyberspace is threatening U.S. national security and economic prosperity."
Source: Joe Biden, "National Cybersecurity Strategy," pg 3.

Recommendations

	Recommendations	Sub-Elements
1	Appoint a Cyberspace Lead and Establish a Supporting Governance Structure to Shape the Cyberspace Domain	1a: Appoint a National Cyber Director with the expanded authorities 1b: Establish a governance structure to shape the cyberspace domain 1c: Invest in emerging technology that enables the US to out-compete authoritarian actors within cyberspace
2	Cultivate Relationships with the Private Sector to Build Cyber Resilience	2a: Enact mandatory disclosure legislation going beyond Cyber Incident Reporting for Critical Infrastructure Act of 2022 2b: Establish a non-DoD Cyber Reserve Force 2c: Establish a Federal "Hack Us" Program through the ONCD and CISA 2d: Establish a Department of Education hub of evidence-based resources to improve information understanding, critical thinking, and digital and media literacy 2e: Enact bipartisan legislation to protect Americans from malign CIO and cyber activity 2f: Establish social media content ratings that include warnings
3	Shape the Federal Government to Take Bold Action	3a: Petition the President to publish an EO delegating authority to Commanding General, USCYBERCOM, to engage in OCOs on behalf of the US 3b: Increase end strength of CNMF and equip with requisite resources to engage adversaries, at scale, in and through cyberspace 3c: Prioritize: 1) persistent engagement with defend forward and 2) integrated deterrence, including OCO to deter, disrupt, and destroy malicious cyber activity

Table 1. Recommendations

Recommendation 1: Appoint a Cyberspace Lead and Establish a Supporting Governance Structure to Shape the Cyberspace Domain

Recommendation 1a: Appoint an NCD with the expanded authorities to synchronize and integrate US efforts to shape the cyberspace domain through strategy and policy.

The US President and Senate must immediately appoint and confirm a NCD to fill the current vacancy. The NCD authorities in 6 U.S.C. § 1500 (2021) must be revised to allow the NCD to synchronize and

integrate cyberspace strategy and policy across relevant Federal entities (i.e., Department of Commerce, DoD, DHS, DoJ, DoS, Office of the National Intelligence Director).¹⁵¹ While 6 U.S.C.

Figure 21. Information and cyber warfare
Source: Bob Gourley, "We Have a Cyber Czar, and He Has Spoken," CTO Vision, (January 30, 2009).

§ 1500 (2021) states the NCD will serve as the lead in the coordination and implementation of national cyber strategy and policy, the NCD lacks the authority to direct and instead “coordinates with” and “provides recommendations to” relevant Federal entities.¹⁵² This shortcoming resulted in the 2023 NCS's singular focus on advancing cybersecurity and reliance on supplemental strategies from relevant Federal entities (e.g., the DoD's USCYBERCOM) to address gaps such as employing more OCO and countering malign CIOs.

OIE Takeaway

Mastering disruptive technologies is the advantage in strategic competition.

The NCD is best positioned to synchronize and integrate US efforts to shape the cyberspace domain through strategy and policy holistically. The existing ONCD aims to advance national security, economic prosperity, and technological innovation through cybersecurity policy and leadership.¹⁵³ Moreover, the ONCD already works closely with White House and interagency partners, all levels of the government, America's international allies and partners, non-profits, academia, and the private sector to advise the President while shaping and coordinating federal cybersecurity policy.¹⁵⁴ The NCD must broaden the aperture of the 2023 *National Cybersecurity Strategy* to holistically address national security threats in the entirety of the cyberspace domain.

Recommendation 1b: Establish a governance structure to shape the cyberspace domain.

The distinct division between the FBI, CISA, state and local cyber defense (all of whom only engage in defensive operations), and USCYBERCOM (which engages defensively and offensively) is stark, and clearly understood but problematic. Most of the USG is in the untenable situation of doing endless defense, which shifts from inadequate to excellent like a sine wave over time.

OIE Takeaway

Democracy distributes the power to process information and make decisions among many people and institutions, whereas dictatorship concentrates information and power in one place. AI may swing the advantage toward the latter.

The NCD already has the authority to coordinate with relevant Federal entities to monitor and assess the effectiveness, including cost-effectiveness, of implementing national cyber strategy and policy.¹⁵⁵ Additionally, the NCD provides advice and consultation to the National Security Council (NSC).¹⁵⁶ However, the US lacks central management of the cyberspace domain. To holistically address cyberspace domain threats, disparate Federal entities must be directed to report to the ONCD their progress toward implementing national cyber strategy and policy. The NCD must urgently establish a working group to inform a holistic *National Cyberspace Strategy*, which reports to the NSC

Figure 22. Cyber Diplomacy Act
Source: Cynthia Brumfield, “Cyber Diplomacy Act Aims to Elevate America’s Global Cybersecurity Standing,” CSO Online, February 25, 2021.

and monitors and assesses the implementation of the *National Cyberspace Strategy*. The Cold War US Interagency Active Measures Working Group provides a good model. This working group played a critical role in collecting and analyzing the information gathered from CIA reporting, FBI investigations, and reports from the US Information Agency overseas posts, which merged with

the DoS, to detect and expose Soviet propaganda and disinformation efforts collectively. The Cyberspace Working Group, led by the NCD, could collect and analyze cyberspace threat information to develop effective strategies and policies while making meaningful recommendations to the NSC. This will allow the White House to expand its approach beyond cybersecurity to shape the cyberspace domain.¹⁵⁷

Recommendation 1c: Invest in emerging technology that enables the US to out-compete authoritarian actors within the cyberspace domain.

The NCD is directed to understand and deter malicious cyber activity and to maintain awareness and direct the adoption of emerging technologies that can improve the US cybersecurity posture.¹⁵⁸ The threat landscape in the cyberspace domain is becoming more challenging with emerging technologies. The ONCD and Cyberspace Working Group must partner with academia and the private sector to develop and employ innovative solutions to counter these threats. In addition to new technology and tools, research can improve understanding the effects of emerging technologies on society (e.g., influence and manipulation) and ways to build resilience to adverse political, societal, and economic outcomes. In the short term, better technology and tools should enhance the ability to identify and address threats surrounding AI, bots, deep fakes, and malign CIOs on social media platforms. In the long term, the US must move towards zero trust frameworks and research the benefits of state-led “tokenized access” to the internet. To shape the cyberspace domain, the US should invest in research and development which focuses on the following:

- The US must develop automated tools to recognize and flag AI, bots, deep fakes, and malign CIOs. The Defense Advanced Research Projects Agency should tackle this challenge, as they are designed to address national security challenges and are typically well-funded. (short-term)
- Social media operators should adopt digital verification methods (e.g., blockchain technology) to guarantee content accuracy. (short-term)
- The US must partner with academia and the private sector to better understand emerging technologies’ effects on human cognition and develop solutions that build societal resilience to adverse political, societal, and economic outcomes. (long-term)
- The US must research ways to incentivize a state-run identification system with a digital key for “tokenized access” to the internet. Tokenized access enables escalating cybersecurity functions such as improving attribution. Tokenized access would open the door for future cybersecurity improvements, such as enforcing “cyber lockout periods” for cyber criminals’ digital access. (long-term)

Recommendation 2: Cultivate Relationships with the Private Sector to Build Cyber Resilience

Recommendation 2a: Mandatory Disclosure – The USG should enact legislation going beyond the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).

Approximately 90 percent of all US infrastructure is privately controlled, and 95 percent of critical infrastructure is private.¹⁵⁹ The CIRCIA requires covered critical infrastructure entities to report pre-determined cyber incidents to CISA within 72 hours of occurrence identification.¹⁶⁰ While CIRCIA enables better awareness and shortens response time, it targets only the 16 critical infrastructure entities.

The USG should enact legislation requiring infrastructure-related firms to disclose all cyber incidents and intrusions within 72 hours to a designated body like the Information Security Analysis Center (ISAC).¹⁶¹ The ISAC would receive and oversee the reports and be responsible

Figure 23.

Source: Thato Menyatso, “Public and Private Sector Security: Better Protection by Collaboration – Augmenta Cyber Security,” Augmenta Cyber Security, March 21, 2022.

for producing widely disseminated public reports. CISA should codify information with ISAC for distribution to rapidly disseminate information to thousands of critical infrastructure owners and operators.

As an example of effective legislation, California’s 2002 breach notification law requires businesses to notify affected individuals when unauthorized parties acquire personal data.¹⁶² As a result, entities have increased awareness of the risks of losing personal data and have invested in preventative measures.¹⁶³

Recommendation 2b: Establish a non-DoD Cyber Reserve Force.

A non-DoD Cyber Reserve Force like the proposed military Digital Reserve Force comprised of private sector experts with linkages and lines of authority to USCYBERCOM and the NSA would improve public-private partnerships, build surge capacity during the conflict, and harden the overall cyberattack surface. Delegated “hack back” authority across the private enterprise through the Cyber Reserves will likely reduce the frequency of cyberattacks by imposing costs on attackers. A *Cyber Letter of Marque* will allow organizations in the private sector to apply for a letter to watch cyberspace outside its network for possible attacks, prevent attacks, and anticipate or respond to attacks. The information gathered would be shared in real-time with Federal authorities. The authority of the letter of marque would be granted after proper vetting of the applicant and be limited in time, scope, location, and duration.¹⁶⁴ The primary obstacle to expanding DoD cyber capabilities to the private sector is the private sector’s unwillingness to accept new authorities. Private sector firms must be incentivized or compelled to accept these authorities through legislation.

OIE Takeaway

Online behavior is dominated by "homophily"—the tendency to listen to and associate with people like yourself, and to exclude outsiders. The power of social media, likewise, is used to intensify nationalism and demonize the enemy. In this strategy, homophily is not something to be feared or avoided by autocracies. It is the goal.

Recommendation 2c: Establish a Federal “Hack Us” Program through the ONCD & CISA.

Google’s Vulnerability Reward Program rewards anyone that finds vulnerabilities in the company’s system¹⁶⁵ – an example of economic incentives that improve security. Private firms should consider hosting “Hacker Capture the Flag” with a similar concept. With tax incentives, the USG could encourage more private sector companies to reward those identifying vulnerabilities within their systems, ultimately making the online environment more secure.

Recommendation 2d: Establish a Department of Education hub of evidence-based resources to improve information understanding, critical thinking, and digital and media literacy inclusive of K-12 and incentivize adult learning.

In addition to funding and compiling research, the US Department of Education should provide financial incentives to states providing media literacy programs per national standards, starting with K-12 grade levels, and include resources for adult continuing education. Education reform across the K-12 grade levels will assist students in recognizing nefarious cyber activity and becoming more resilient to cyberattacks and malign IO.

Federal initiatives such as The Literacy Information and Communication System and the Digital Equity Accelerator already build capacity and societal resilience in the information environment

Figure 24.

Source: Jeff Edwards, “I Want You! ... To Hack the US Army,” Best Endpoint Protection Security (EPP) Tools, Software, Solutions & Vendors, November 15, 2016.

but have limited reach. The Federal role in education is limited by the US Constitution, which

delegates educational decisions to local levels and subjects them to local partisan political debate. This myopic approach to education limits students' digital literacy education opportunities. Political disagreement can be mitigated by developing resources focusing on understanding and identifying threats in every community.

Recommendation 2e: Enact bipartisan legislation to protect Americans from malign CIO and cyber activity.

Congress must enact bipartisan legislation that better protects the American people from malign CIO and cyber activity. The following are new or proposed areas of consideration that are yet to be enacted.

- **Mandatory Bot Disclosure Law.** To protect the American people from malign IO using AI, the USG should pursue legislation that requires the identification of AI and social media bots. For example, the law could require mandatory disclosure when a bot is in use to increase transparency to the consumer. California passed a bot disclosure law, California Business and Professions Code § 17940, effective July 1, 2019.¹⁶⁶ The California legislature emphasized consumers' rights to know when they are speaking to "a real person or a piece of software."¹⁶⁷ Companies must disclose the bot in a "proactive, clear, and conspicuous ... [manner when] ... used to incentivize a purchase or sale of goods or services in a commercial transaction or to influence a vote in an election."¹⁶⁸ Additionally,

Figure 25. Bot Disclosure

Source: "Not Even Bots Are Safe From California Law Makers," epiq, (2019).

the USG should provide tax incentives to social media firms that are innovating to reduce the number of social media bots on their platforms.

- **Protect the Nation's most Precious Resource.** Enacting the recently proposed Protecting Kids on Social Media Act would set a minimum age of 13 to use social media apps and require parental consent for 13 through 17-year-olds. The bill would also prevent social media companies from feeding content using algorithms to users under the age of 18.¹⁶⁹

Figure 26. Protecting Kids on Social Media

Source: "New US Senate bill bans social media accounts for children under 13," abc11 Technology, (April 27, 2023).

Recommendation 2f: Establish social media content ratings that include warnings.

The USG should incentivize social media firms to create a central body that determines ratings for social media content or identifies content that might be controversial, e.g., sexually explicit, graphic, profane, or false. It could be modeled after the movie industry's Motion Picture Association of America or the Entertainment Software Rating Board for the video game industry. It could also be modeled after the television content rating system that was developed cooperatively but is implemented voluntarily.¹⁷⁰

Recommendation 3: Shape the Federal Government to Take Bold Action

Recommendation 3a: The President should issue an Executive Order (EO) delegating authority to the Commanding General, USCYBERCOM, to engage in OCO on behalf of the US.

Attempts to deter malicious actors in cyberspace through unsupported threats of consequence, law enforcement action, and diplomatic measures are ineffective in shaping the cyber behavior of US adversaries. To date, the US has limited its responses to cyberattacks due to the risks of escalation, international backlash, and limited effects. That risk is disputable, and cyberattacks during competition have not escalated to armed conflict. The US will require more offensive actions and responses to threat actors to achieve effects at scale, disrupting and dismantling cyber threat activity at its source. When the US takes this required step, the support of allies, partners, and the remainder of the international community will follow.

OCO will include proportional responses, including appropriate escalation, and will be in response to cyberattacks below the threshold of armed conflict. Responses will authorize integrated deterrence across all domains and emphasize interagency coordination. Justification for EO rests on national security interests in the absence of established norms, lack of customary international law, and nonexistent treaties with adversaries.

The cyber deterrence posture conceived by President Bush and currently employed by President Biden has not reduced or stopped influence, ransomware, theft of IP, or strategic competition. The deterrence strategy requires restraint on behalf of the US and is only practical with those parties that agree with select norms. The US cannot continue to operate in this way.

Recommendation 3b: Increase end strength of CNMF and equip it with requisite resources to engage adversaries, at scale, in and through cyberspace.

CNMF plays a role in maintaining the integrity of state, local, and Federal elections and has the authority to conduct missions to counter malicious cyberspace actors. Despite its recent establishment as a sub-unified command, CNMF needs to be bigger to counter the volume and frequency of attacks on the public and private sectors in the US. Title 10 authorizes the legal basis for the DoD to conduct its operations, yet the capabilities to conduct OCO are limited to a very small military organization. To increase effectiveness, the organization must grow exponentially. The cost to grow the CNMF will come at the reduction in the end strength of other DoD organizations; however, the current battle for dominance in cyberspace, which impacts all other domains, justifies bold steps.

Figure 27.

Source: "Air Force Cyber Mission Force Teams Reach 'Full Operational Capability,'" Schriever Space Force Base (Archived), accessed May 19, 2023.

Recommendation 3c: In the forthcoming DoD Cyber Strategy, prioritize: 1) persistent engagement with "defend forward" and 2) integrated deterrence, including OCO, to deter, disrupt, and destroy

malicious cyber activity at its source. Fortify and protect critical infrastructure that supports the cyberspace domain deemphasizing reliance on deterrence.

The DoD Cyber Strategy should embrace and develop the strategy of persistent engagement at scale. Persistent engagement combines defending forward, contesting, and countering malicious actors with resiliency and is a proven strategy that degrades actors' capabilities.¹⁷¹ Persistent engagement at scale will allow US cyber forces to shape cyberspace during competition and conflict.¹⁷² Persistent engagement, on the other hand, lends itself to competition, eventually leading to norms that will result in expected behaviors and expected consequences.¹⁷³

Integrated deterrence employs all elements of national power and can be employed in all domains. Integrated deterrence has few limitations and can incorporate emerging technologies and other advancements to maintain a US decisive advantage in all phases of competition.

Conclusion

Globalization has created a world in which everything has become a tool for competition – most especially cyberspace, speech, and IO. The US narrowed focus on cybersecurity and defense has led to a comparative disadvantage. Adversaries see cyberspace as a poorly defended domain where the US can be weakened and undermined through strategic competition below armed conflict. The US is timid in conducting offensive operations to defend norms; it is committed to the laws of armed conflict and established international norms involving sovereignty. As a result, Russia and China take advantage of the US's self-imposed restraint. Putin's Russia interferes in our elections and manipulates information by exploiting fissures in our social fabric to influence opinion and decision-making. Putin's foreign policy seeks to advance chaos and dissension within the US. By inundating US cyberspace with divisive material, a gordian knot of competing information overwhelms the end user and advances Putin's foreign policy goals. China has established totalitarian control over the information environment and cyberspace domain within its borders and seeks to export that level of control through technological capabilities, economic influence, and selling its surveillance apparatus abroad.

Figure 28.

Source: Yukihiro Sakaguchi, "U.S. Hosts Global Talks on China, Russia Cyber Threats," Nikkei Asia, October 13, 2021.

Cyber challenges are evolving and never complete. The US must lead the change in cyberspace operations to reduce economic espionage, IP theft, ransomware attack, and information manipulation while advancing OCOs, intelligence collection, and economic competitiveness. Bold action will shape cyber behavior and lead to a stable and reliable cyberspace domain while advancing US national interests and democratic values.

Figure 29. LOEs for Improving Strategic Competition in the Cyberspace Domain (OIE Industry Study Recommendations)

Annexes

Annex A - Acronyms

AI	Artificial Intelligence
APT41	Chinese hacking group
CCP	Chinese Communist Party
CIA	Central Intelligence Agency
CIRCA	Cyber Incident Reporting for Critical Infrastructure Act
CIO	Cyber Information Operations
CISA	Cybersecurity and Infrastructure Security Agency
CNMF	Cyber National Mission Force
DIMEFIL	Diplomatic, Informational, Military, Economic, Financial, Intelligence, & Law Enforcement.
DHS	Department of Homeland Security
DNC	Democratic National Committee
DoD	Department of Defense
DoJ	Department of Justice
DoS	Department of State
EO	Executive Order
ESG	Election Security Group
EU	European Union
FBI	Federal Bureau of Investigation
FSB	Federal Security Service (Russia)
FSO	Federal Protective Service (Russia)
GEC	Global Engagement Center
GRU	Main Directorate of the General Staff (Russia)
HHS	Department of Health and Human Services
IO	Information Operations
IP	Intellectual Property
IRA	Internet Research Agency (Russia)
LOE	Level of Effort
NATO	North Atlantic Treaty Organization
NCD	National Cyber Director
NCS	National Cybersecurity Strategy
NSA	National Security Agency
NSC	National Security Council
OCO	Offensive Cyber Operations
OIE	Operations in the Information Environment
ONCD	Office of the National Cyber Director
ONID	Office of the National Intelligence Director
PLA	People's Liberation Army

PPD	Presidential Policy Directive
PRC	People's Republic of China
SSF	Strategic Support Force (China)
SVR	Foreign Intelligence Service (Russia)
US	United States
U.S.C.	US Code
USCYBERCOM	US Cyber Command
USG	United States Government

Annex B – Key Cyber Competition Terms

Overall

1. **Cyberspace:** A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 3-12)
2. **Cyber power:** The ability to use cyberspace to create advantages and influence events in all operational environments and across the instruments of power. Cyber power is unique in that it is a core element of all the instruments of power: Diplomatic, Informational, Military and Economic (DIME).
3. **Cyber strategy:** Strategies that enable and exploit the capabilities that cyberspace offers while protecting and defending against the vulnerabilities it simultaneously presents.
4. **Gray zone:** Coercive approaches that may fall below perceived thresholds for US military action and across areas of responsibility of different parts of the USG.
5. **Zero trust frameworks:** A security model that encompasses, 'never trust, always verify.'

Information Operations

6. **Propaganda:** The propagation of an idea or narrative that is intended to influence, similar to psychological or influence operations. It can be misleading but true and may include stolen information. A government communicating its intent, policies, and values through speeches, press releases, and other public affairs can be considered propaganda.
7. **Misinformation:** false information, spread not necessarily with the intent to deceive.
8. **Disinformation:** false information, known to be false, deliberately spread to influence or obscure the truth.
9. **Disinformation Campaign:** A systematic government effort using disinformation to mislead a particular audience in order to influence the policy process.”
10. **Information Warfare:** A strategy for the use and management of information to pursue a competitive advantage, including both offensive and defensive operations.
11. **Retorsion:** ‘Retorsion’ is what signals acceptable and unacceptable activity. Retorsion refers to the taking of measures that are lawful but unfriendly, directed against another State. Retorsion may therefore be used regardless of whether international law has been violated and regardless of whether State responsibility applies.

Deterrence

12. **Cross-domain deterrence:** A capability in one domain that constrains adversary behavior through the denial of benefits or the imposition of costs on an adversary's selected course of action in another domain.
13. **Integrated deterrence:** A new deterrence model that intends to expand the nuclear deterrence paradigm and constructs deterrence regimes across all domains and across the spectrum of competition by leveraging all instruments of national power, dominating the information space, and advancing cross-domain deterrence across all Combatant Commands. It involves allies and partners and harnesses emerging technologies and concepts, such as quantum computing and artificial intelligence.

China

14. **Informatized Warfare:** The process of acquiring, transmitting, processing, and using information to conduct joint military operations across the domains of land, sea, air, space, cyberspace, and the electromagnetic spectrum during a conflict; the use of information technology to create an operational system-of-systems to enable the PLA to acquire, transmit, process, and use information during a conflict to conduct joint military operations across the ground, maritime, air, space, cyberspace, and electromagnetic spectrum domains.
15. **Digital Authoritarianism:** The use of digital information technology by autocratic governments to surveil, repress, and manipulate domestic and foreign populations; it has six major techniques that allow authoritarians to decrease trust in public institutions, increase social and political control, and/or undermine civil liberties: surveillance, censorship, social manipulation and harassment, cyber-attacks, internet shutdowns, and targeted persecution against online users.

Russia

16. **Hybrid warfare:** A mixture of unconventional tactics and strategies, irregular forces, covert action, cyber operations, and political manipulation to achieve strategic goals; a collection of tactics designed to circumvent deterrence and avoid military retaliation by skirting the threshold of what could be considered state use of armed force. In this new style of conflict, non-kinetic actions can be as important as kinetic attacks.
17. **Troll Farm:** Russia is the birthplace of a new, secretive, state-sponsored industry (Government-sponsored social media propagandists) designed to spread pro-Russian propaganda, attack government critics, and sow domestic distrust about the internet.

Annex C – OIE Industry Study Engagement and Speakers

<u>Location</u>	<u>Date</u>	<u>Who</u>
Virtual	02/16/23	Dr. Jennifer Golbeck, Professor, College of Information Studies, University of Maryland
Virtual	02/23/23	Professor Daniel Silverman, Institute for Politics & Strategy, Carnegie Mellon University
Virtual	02/24/23	Dr. Scott Jasper, Naval Postgraduate School
NY	03/02/23	Mr. Amit Kachhia-Patel, FBI, Supervisory Special Agent
NY	03/02/23	Ms. Kelly Moan, NYC CISO, The NYC Office of Technology & Innovation
NY	03/02/23	Mr. Chris DeSain, NY CISO, The New York State Office of Information Technology Services
NY	03/02/23	Ms. Rebekah Fisk, Director, Education, The Paley Center for Media
NY	03/03/23	Mr. Mohamed Telab, Deputy Regional Director, Region 2: NY, NJ, PR and USVI, Cybersecurity and Infrastructure Security Agency (CISA)
NY	03/03/23	Mr. David Shafer, Head of Global Security, NASDAQ
NY	03/03/23	Ms. Lee Anne Milhiser, Vice President and Head of Global Enterprise Risk Management, NASDAQ
NY	03/03/23	United Nations, 2023 Cyber Stability Conference
Classroom	03/07/23	Mr. Charley Snyder, Head of Security, Google
Virtual	03/09/23	Mr. Chris Rose, NATO, CISA Briefing
DC, virtual	03/16/23	Mr. Matthew Ferren, Assistant National Cyber Director for Strategy & Research, Office of the National Cyber Director, Executive Office of the President
DC, virtual	03/16/23	Ms. Kseniya Kirillova, journalist and author
DC, virtual	03/17/23	Mr. Matt Altomare, Planner, Cyber Operations Section, Joint Cyber Defense Collaborative, Planning Office, CISA
DC	03/16/23	The Spy Museum, “History of SIGINT and Cyberspace”
DC	03/17/23	Global Engagement Center, Department of State
Campus	03/22/23	NDU Cyber Summit
Latvia	03/27/23	Mr. Ambassador Christopher Robinson, US Ambassador to Latvia
Latvia	03/27/23	Dr.sc.pol. Ieva Bērziņa, Senior researcher, The National Defence Academy of Latvia Center for Defence Research
Latvia	03/27/23	Mr Rolands Henriņš, Undersecretary of State-Policy Director (MOD round table)
Latvia	03/27/23	Mr Kaspars Galkins, Director of Public Affairs Department (MOD round table)
Latvia	03/27/23	Mr Edgars Kiukucāns, Director of the National Cybersecurity Policy Department (MOD round table)
Latvia	03/27/23	NATO’s Centre of Excellence for Strategic Communications

Latvia	03/27/23 Mr. John Sunderland, NATO Stratcom
Estonia	03/28/23 Lt Col Graham Price, NATO Cooperative Cyber Defence Centre of Excellence ('CCDCOE')
Estonia	03/28/23 Mr. Mark Riisik, Estonian Ministry of Defense, Security
Estonia	03/28/23 e-Estonia Briefing Centre
Estonia	03/28/23 Mr. Jaak Tarien, Cybernetica
Estonia	03/28/23 Mr. Mihkel Tikk, Deputy Commander at Estonian Defence Forces Cyber Command
Estonia	03/28/23 Mr. Harrys Puusepp, Head of Bureau at Estonian Internal Security Service (KAPO)
Estonia	03/28/23 Mrs. Kersti Luha, Head of Strategic Communication at the Government Office
Estonia	03/28/23 Col Uku Arold, Deputy Chief of Estonian Defence Forces Strategic Communications
Estonia	03/28/23 Mr. Ambassador George Kent, U.S. Ambassador to Estonia Dr. Pablo Breuer, CISO, Helm Services
Finland	03/30/23 The European Centre of Excellence for Countering Hybrid Threats
Finland	03/30/23 National Defense University, National Cyber Security Center: Lehtila Olli, Sauli Pahlman, Pekka Jokinen, Stefan Lee
Finland	03/30/23 Vesa Kekale, Ministry of Foreign Affairs, Countering Hostile Threats
Finland	03/30/23 LTC Tuomas Liukko, National Defense University
Finland	03/30/23 Professor Miina Kaarkoski, National Defense University
Finland	03/31/23 Mr. Christian Perheentupa, Security Committee
Finland	03/31/23 Mr. Antti Sillanpää // NESA (National Emergency Supply Agency)
Finland	03/31/23 Mr. Otto Saxén, Ministry of Defense
Finland	03/31/23 LTC Timo Hänninen, DEFCOM (J5)
Finland	03/31/23 Mr. Ambassador Doug Hickey, U.S. Ambassador to Finland
CA	04/11/23 Dr. Jacquelyn Schneider, The Hoover Institution, Stanford University
CA	04/11/23 Mr. Joe Felter, Center Director, Stanford University, Gordian Knot Center for National Security Innovation
CA	04/11/23 Hacking 4 Defense class observation, Stanford University
CA	04/12/23 Mr. Stephan Somogyi, Product Manager, Counter Abuse Technologies, Google Cloud Space
CA	04/12/23 Mr. Royal Hansen, Vice President of Privacy, Safety and Security Engineering, Google Cloud Space
CA	04/12/23 Mr. Courtney Chapman, Google

		Cloud Space
CA	04/13/23	Assistant Professor Ryan Maness, Naval Postgraduate School
CA	04/13/23	Professor Emeritus John Arquilla, Naval Postgraduate School
Classroom	04/18/23	Mr. JJ Green, WTOP
Classroom	04/25/23	Mr. Gary Brown, Professor, The Eisenhower School for National Security and Resource Strategy
DC	05/01/23	U.S. Agency for Global Media: Ms. Mirela Bruk; Ms. Karine Roushanian; Mr. Alen Mlatishuma, Eurasia Division; Ms. Sandra Lemaire, Latin America Division; Ms. Tori Tsui, Asia Fact Check Lab; Mr. Martins Zvaners, Deputy Director, External Affairs; Mr. Chad Hurley, Director, Office of Internet Freedom; & Ms. Amanda Bennett, CEO, US Agency for Global Media; Voice of America: Ms. Jodi Reed

NDU Presidential Lecture Series Relevant to Cyberspace

<u>Date</u>	<u>Who</u>
01/04/23	General Paul Nakasone (CDR, United States Cyber Command)
02/04/23	General Glen D. Van Herck (CDR, NORTHCOM/NORAD)
03/01/23	Dr. Colin H. Kahl Under Secretary of Defense for Policy
04/05/23	General Jacqueline Van Ovost (CDR, USTRANSCOM)

As a program, Presidential Lecture Series (PLS) events allow an NDU-wide audience to benefit from the perspectives and experience of distinguished leaders from the military services, various government departments/agencies, as well as the international community and private industry. The theme for the PLS is updated as needed to ensure relevance with evolving joint learning objectives and Special Areas of Emphasis promulgated by the Chairman of the Joint Chiefs of Staff.

ES Commandant Lecture Series Relevant to Cyberspace

<u>Date</u>	<u>Who</u>
01/11/23	Mr. Mike Madsen (Acting Director of DoD's Defense Innovation Unit)
01/18/23	U.S. Space Force Panel Discussion (MGs Gagnon and Whitney)
03/14/23	General (Ret.) Stephen Lyons, (Former CDR, USATRANSCOM)

03/22/23

General (Ret.) Norton Schwartz (Former Chief of Staff, Air Force)

The Commandant Lecture Series (CLS) complements core courses by bringing in highly distinguished military officers, government officials, security practitioners, academics, and industry executives to share their unique perspectives in leadership and national security. Through prepared remarks by speakers and interactive Q&A sessions, Eisenhower students are provided personal interactions with leaders who are shaping the national and international security environment.

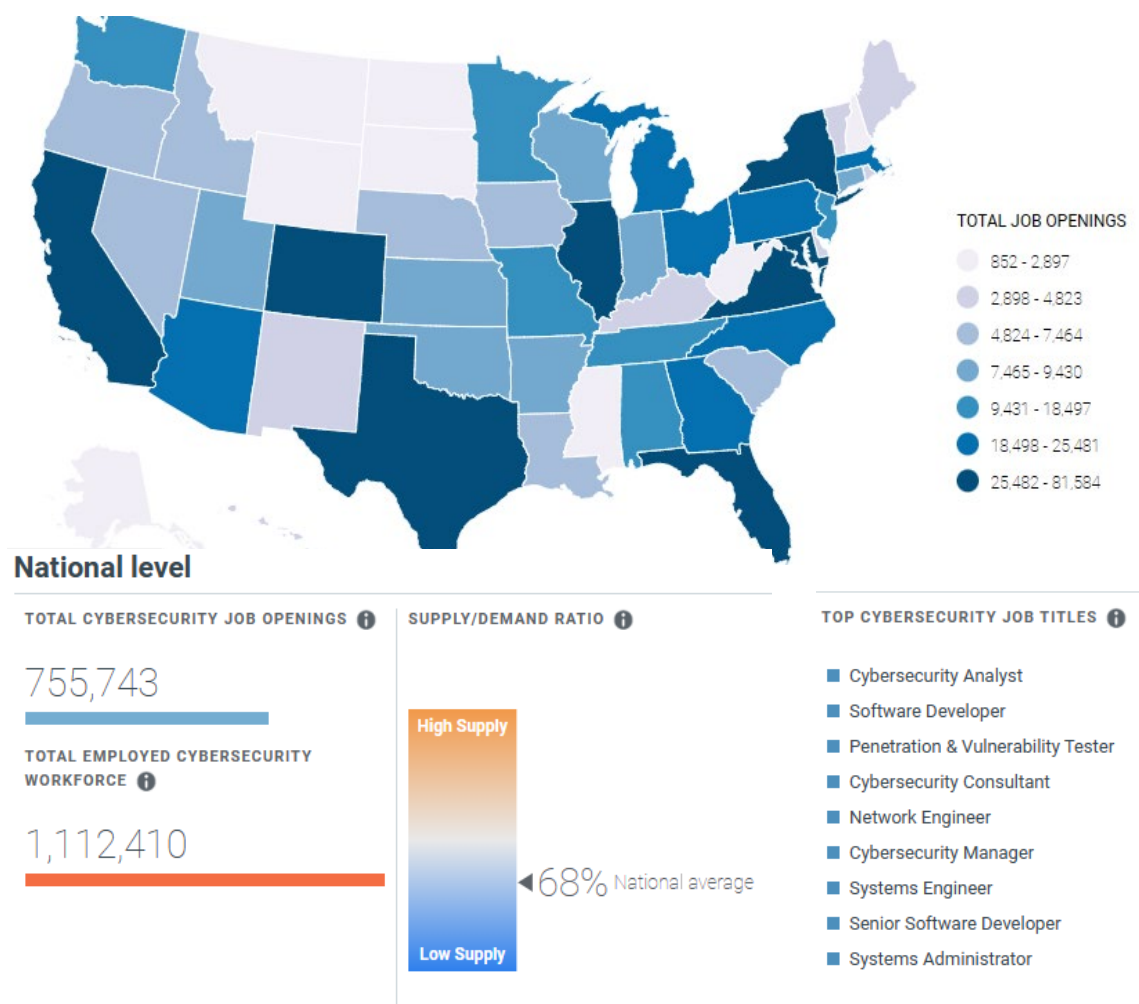
Map of OIE Industry Study Locations Visited

Annex D – Cyber Employees

Cyber Employees

While over one million US employees comprise the cybersecurity workforce to combat and defend against cyber-attacks, that population only fills 68 percent of the demand.¹⁷⁴ There are over 700,000 cybersecurity job vacancies in the US alone (see below).¹⁷⁵ Worldwide, at least 2.7 million more professionals are required for cybersecurity.¹⁷⁶ With individuals and private and public sector entities moving from the analog to the digital world, that demand will only increase.

Figure. Current US Cybersecurity Specialist Supply/Demand Heat Map



American school students are the targeted population to eventually fill the vacant and growing cyber positions domestically, but access to the internet for all school students remains a challenge. Digital literacy cannot bloom unless American children nationwide have digital equity, defined as equal access to the tools required to navigate as citizens in a digital world. Tools include internet access and devices such as computers and tablets. In 2022, more than ten percent of US households had no internet access.¹⁷⁷ That equates to over 30 million citizens (about the population of Texas)

without internet at home or a network device. Comparatively, Finland, the nation with the highest digital literacy rate, also has a household access rate of almost 98%.¹⁷⁸

Demographic distribution of internet access paints a troubling picture. A recent study by the US Department of Education found that 40 percent of students in K-12 identify as Black, Hispanic, or Native American, but 54 percent lack internet access or computers at home.¹⁷⁹ Lack of access is a significant socioeconomic problem that negatively impacts students' opportunities and the development of a potential pool of cyber talent.

The current Head of the Estonian Cyber Olympics Talent Program, Dr. Birgy Lorenz, stated, "The sustainability of every digital country depends on our ability to harness the competence of the young people."¹⁸⁰ She is not alone in her sentiment. A safety and security section member in a major American global search engine company said that to find the source of most security breaches in the cyber world, look for "Advanced Persistent Teenagers."¹⁸¹ He then explained how teenage girls were the "state-of-the-art" on situational awareness in the cyber world, with survival adaptations we are not tapping into but should.¹⁸²

In addition to the lack of cyber education and talent development, the US must appropriately frame the cyberspace domain. Cyberspace is often characterized inaccurately as an unlimited, incomprehensible domain that confounds rational analysis for policy creation. Establishing stability in cyberspace is the goal, where economic activity progresses without widespread fear of attack and criminals and repugnant state actors are held accountable. Eventually, the cyberspace domain will reach stability, given the action and reaction behavior between the provocateurs and defenders. In the years before natural stability occurs, the fortunes of nations will rise and fall, incentivizing the United States, as the current leader in prosperity, to hasten the approach to peace through creative policies.

One critical difference between the land and cyberspace domains is cyber's rapid evolution. Most police work involves similar crimes conducted under similar methods under similar motives. As noted by a cybersecurity expert at a leading US technology company, the rapid advances in cybersecurity create an arms race for adversaries to innovate new attack methods.¹⁸³ Key to US success moving forward in cyberspace is understanding specific nation-states and threat types and how they employ tactics, techniques, and procedures.

Annex E – Tables and Figures

Figure #	Figure Title	Source	Page #
1	“Best Friends?”	Heather A. Conley et al., “Countering Russian & Chinese Influence Activities,” www.csis.org , July 1, 2020, https://www.csis.org/analysis/countering-russian-chinese-influence-activities-0 .	1
2	The Information Environment	Department of Defense Joint Staff, “Joint Publication 3-13, Information Operations,” November 20, 2014, I-2, https://irp.fas.org/doddir/dod/jp3_13.pdf .	3
3	Information Warfare: Issues for Congress	Catherine A. Theohary, “Information Warfare: Issues for Congress,” March 5, 2018, 5, https://crsreports.congress.gov/product/pdf/R/R45142 .	3
4	Three Interrelated Layers of Cyberspace	Department of Defense Joint Staff, “Joint Publication 3-12, Cyberspace Operations,” June 8, 2018, Figure I-1, I-3, https://irp.fas.org/doddir/dod/jp3_12.pdf .	4
5	Cyberthreat Real-Time Map of attacks taken in a one-second timeframe on May 18, 2023	“MAP Kaspersky Cyberthreat Real-Time Map, 2018, https://cybermap.kaspersky.com/ .	5
6	US Cyber Command Activated	“Gates establishes US Cyber Command, names first commander,” Air Force News, (May 21, 2010), https://www.af.mil/News/Article-Display/Article/116589/gates-establishes-us-cyber-command-names-first-commander/ .	7
7	Defending Forward	Robert Chesney, “The 2018 DoD Cyber Strategy,” Lawfare, (September 25, 2018), https://www.lawfareblog.com/2018-dod-cyber-strategy-understanding-defense-forward-light-ndaa-and-ppd-20-changes .	7
8	Social Media Across the Globe	Colm Russell, “Social Media Recruitment – Driving Change for International Data Collection,” Dynamic Fieldwork, accessed May 11, 2023, https://www.dynamicfieldwork.com/social-media-recruitment/ .	8
9	Number of Social Media Users in the US from 2019 to 2028 (in millions)	Statista, “U.S. Number of Social Media Users 2023 Statista,” Statista (Statista, 2017), https://www.statista.com/statistics/278409/number-of-social-network-users-in-the-united-states/ .	9
10	Social bots	Nick Bilton, “Social media bots offer phony friends and real profit,” The New York Times, (November 19, 2014), https://www.nytimes.com/2014/11/20/fashion/social-media-bots-offer-phony-friends-and-real-profit.html .	10

11	General Nakasone	Amy McCullough, “Ukraine Crisis to Influence Growth of US Cyber Force, Nakasone Says,” Air & Space Forces Magazine, April 6, 2022, https://www.airandspaceforces.com/ukraine-crisis-to-influence-growth-of-us-cyber-force-nakasone-says/ .	11
12	Total Facebook engagements for the top 20 election stories	Lt Col Jarred Prier, “Commanding the Trend: Social Media as Information Warfare,” Strategic Studies Quarterly Vol. 11, no. 4 (Winter 2017): 61, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-11_Issue-4/Prier.pdf .	12
13	Russian Disinformation Modus Operandi	Global Engagement Center, “GEC Special Report: Pillars of Russia’s Disinformation and Propaganda Ecosystem,” US Department of State, August 2020, https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf .	14
14	FBI Wanted Posted for Six Russian GRU Hackers	Andrei Soldatov and Irina Borogan, “Russian Cyberwarfare: Unpacking the Kremlin’s Capabilities,” CEPA, September 8, 2022, https://cepa.org/comprehensive-reports/russian-cyberwarfare-unpacking-the-kremlins-capabilities/ .	16
15	Chinese Soldiers Conducting Information Review and Operations	Remco Zwetsloot, “The US needs multilateral initiatives to counter Chinese tech transfer,” Tech Stream, (June 11, 2020), https://www.brookings.edu/techstream/the-u-s-needs-multilateral-initiatives-to-counter-chinese-tech-transfer/ .	17
16	China’s Firewall	Shira Ovide, “Copying China’s Online Blockade,” The New York Times, (March 1, 2021), https://www.nytimes.com/2021/03/01/technology/copying-chinas-online-blockade.html .	18
17	How China Influences the Globe	Sarah Cook, “Beijing’s Global Megaphone,” Freedom House, (2020), https://freedomhouse.org/report/special-report/2020/beijings-global-megaphone .	19
18	FBI Director Address on China Cyber Threat	Christopher Wray, “The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States,” FBI News, (July 7, 2020), https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states .	21
19	Chinese Military equipment modernized using IP	Raashi Shah Assistant Manager et al., “Global Research and Analytics Firm,” www.aranca.com, September 9, 2020, https://www.aranca.com/knowledge-library/articles/investment-research/ip-theft-china-and-beyond .	21

20	China's Cyberespionage activities since 2006	Yossi, "U.S. Accuses China of Cyber-Spying - Hamodia.com," Hamodia, May 20, 2014, https://hamodia.com/2014/05/19/u-s-accuses-china-cyber-spying/ .	22
21	Information and cyber warfare	Bob Gourley, "We Have a Cyber Czar, and He Has Spoken," CTO Vision, (January 30, 2009), https://ctovision.com/we-have-a-cyber-czar-and-he-has-spoken/ .	24
22	Cyber Diplomacy Act	Cynthia Brumfield, "Cyber Diplomacy Act Aims to Elevate America's Global Cybersecurity Standing," CSO Online, February 25, 2021, https://www.csoonline.com/article/3609518/cyber-diplomacy-act-aims-to-elevate-americas-global-cybersecurity-standing.html .	25
23	Figure 23	Thato Menyatto, "Public and Private Sector Security: Better Protection by Collaboration – Augmenta Cyber Security," Augmenta Cyber Security, March 21, 2022, https://augcyba.com/pubpriv-mrch22/ .	27
24	Figure 24	Jeff Edwards, "I Want You! ... To Hack the US Army," Best Endpoint Protection Security (EPP) Tools, Software, Solutions & Vendors, November 15, 2016 https://solutionsreview.com/endpoint-security/i-want-you-to-hack-the-army/ .	28
25	Bot Disclosure	"Not Even Bots Are Safe From California Law Makers," epiq, (2019), https://www.epiqglobal.com/en-us/resource-center/articles/california-online-bot-law .	29
26	Protecting Kids on Social Media	"New US Senate bill bans social media accounts for children under 13," abc11 Technology, (April 27, 2023), https://abc11.com/impact-of-social-media-on-kids-protecting-act-childrens-health-senate-legislation/13190219/ .	30
27	Figure 27	"Air Force Cyber Mission Force Teams Reach 'Full Operational Capability,'" Schriever Space Force Base (Archived), accessed May 19, 2023, https://www.schriever.spaceforce.mil/News/Article-Display/Article/1529147/air-force-cyber-mission-force-teams-reach-full-operational-capability/ .	31
28	Figure 28	Yukihiro Sakaguchi, "U.S. Hosts Global Talks on China, Russia Cyber Threats," Nikkei Asia, October 13, 2021, https://asia.nikkei.com/Politics/International-relations/U.S.-hosts-global-talks-on-China-Russia-cyber-threats .	32
29	LOEs for Improving Strategic Competition in the Cyberspace Domain		33
Table 1	Recommendations		24

Page intentionally left blank.

HOW TO COUNTER CHINA'S DIGITAL SILK ROAD

(NETWORKING AND MEDIA INDUSTRY STUDY)

Annex F – Digital Silk Road Addendum Paper

*Whereas to date, the United States has treated China's Digital Silk Road (DSR) initiative (the digital subset of China's Belt and Road Initiative) as a cyber sovereignty and espionage concern, China's larger strategy for DSR is most likely to build a "less US-centric and more Sino-centric global digital order."*¹⁸⁴

China's 2015 complement to its Belt and Road Initiative (BRI) – the Digital Silk Road (DSR) -- is designed to garner global influence via infrastructure and services in cyberspace. Its focus includes physical infrastructure, 5G networks, China's BeiDou Global Positioning System (GPS), smartphone applications, and e-commerce. BRI engagement in cyberspace has afforded China a low-cost path to expand economically, politically, and militarily. As of 2018, DSR-related investments internationally equated to \$79 billion.¹⁸⁵ China's BRI will likely continue to shift to less costly and more influential DSR projects.

- The United States characterizes the DSR primarily as a cyber sovereignty and espionage concern; this ignores the full spectrum of China's strategic goal for the DSR, and the global demand China meets in the absence of a US alternative.
- The failure to characterize and address the DSR as a larger strategic concern has likely resulted in a delayed and flawed American response; this endangers long-term economic growth, global norms, and free, open, and secure connectivity.

China's digital infrastructure and surveillance tools advance exploitation and control by autocratic nations. Cuba, Iran, North Korea, Russia, Zimbabwe, and Venezuela employ Chinese cyberspace capabilities to monitor their populations.¹⁸⁶ China also uses DSR infrastructure to conduct influence operations via an international media empire employing state media bureaus, foreign media companies, and overseas partnerships.¹⁸⁷

China's BeiDou navigation system, adopted by 200 countries with one billion users,¹⁸⁸ jeopardizes US market share.¹⁸⁹ China conceptualized BeiDou in 1996, fearing dependence on GPS enabled by the US.¹⁹⁰ BeiDou's greater accuracy cuts into US global navigation market share and furthers DSR expansion as an element of China's total technology package.¹⁹¹ BeiDou's unique 2-way communication capability also enables tracking and surveillance of all devices using the system within range of a ground monitoring station.¹⁹²

DSR weakens US alliances and partnerships. China exploited global dissatisfaction with the US's technology policy limitations under Trump-era protectionist policies, adeptly filling needs for connectivity and infrastructure.¹⁹³ A 2019 study of five US allies found that market access and commercialization outweighed security concerns in adopting Huawei's 5G and the BeiDou

systems.¹⁹⁴ DSR also advances academic exchanges and research partnerships, endangering US emerging technologies through a backdoor to key partners such as Israel.¹⁹⁵

DSR success positions China to set global digital standards. DSR expansion emboldens countries to establish national firewalls, throttle data flow, and censor free expression, advancing autocratic cyberspace norms in the absence of global standards.¹⁹⁶ China is now a leading contributor to the United Nations International Telecommunications Union (ITU) with alleged interests in “strengthening international standards for emerging digital ICT infrastructure.”¹⁹⁷ Beyond challenging the US free and open internet principle, this splinternet reduces access to global markets, hampering long-term economic growth and access to critical information.¹⁹⁸

RECOMMENDATIONS

Expand US influence operations by leveraging open-source reporting on the malign goals of the CCP’s BRI, using a multi-platform approach via online gaming and short-wave radio.

US messaging and counter-messaging should convey to DSR recipient governments the pitfalls of doing business with the CCP through numerous and penetrating media. Since many BRI recipients have limited access to independent media, the United States should attempt to reach larger audiences through new media channels, such as online gaming. There are approximately 2.7 billion gamers worldwide.¹⁹⁹ Publicizing incidents like the African Union’s discovery—and subsequent removal—of China’s backdoor channel to monitor information and communication flow can galvanize domestic audiences and sway policymakers.²⁰⁰ This approach mirrors efforts taken to reach Russians who otherwise only receive Russian owned state propaganda.²⁰¹



Build and deploy ground monitoring stations worldwide to maintain dominance of the US GPS by ensuring data availability.

The United States has built and deployed only 11 ground monitoring stations abroad compared to China’s 120.²⁰² China’s deployment provides positioning, navigation, and timing (PNT) availability worldwide, but particularly in developing countries -- decreasing reliance on US infrastructure and influence. The proliferation of China’s PNT leads directly to increased sales of Chinese infrastructure. Adoption of China’s PNT allows Chinese business to market its highly sophisticated train control systems, precision agriculture equipment, and autonomous driving capabilities.²⁰³

Invest in basic and applied research in advanced technologies such as 6G to pull back market share and establish the United States as the digital partner of choice.

The DOD should prioritize 6G research to maintain its strategic edge and establish the United States as the partner of choice. Future 6G Communication networks must be interoperable so that US firms can wrest back market share. To achieve global 360-degree connectivity in a 3D space, interoperability issues with heterogeneous services, applications, protocols, and networks must be solved.²⁰⁴ Increased investment in key US science and technology agencies, such as the National Science Foundation (NSF) or Defense Advanced Research Projects Agency (DARPA), along with investments by US commercial firms, will help the United States compete with China in advancing next generation technologies.²⁰⁵ Although the US advised countries such as the UK, France, and Canada to ban Huawei due to security concerns, Huawei is still dominant in countless developing markets as well as the substantial Chinese market. That revenue, coupled with China's research institutes, puts Huawei at a significant advantage in the 6G development race, in contrast with Western competitors, who are hampered by market rivalry and limited development funds from their governments.²⁰⁶

Provide aid to advance digital connectivity to those countries assessed to have strategically important assets at risk of further BRI investment.

China has targeted countries suffering from extreme poverty as well as those ineligible for funding from institutions such as the IMF, World Bank, or ASEAN due to human rights violations or corruption. China offers such states its 5G communications as a low-cost model, netting it 70 percent of Africa's digital infrastructure capacity.²⁰⁷ The United States needs to identify those states and provide funding to countries that offer a strategic advantage. One method is through USAID's Digital Invest program, which uses private capital to expand digital connectivity infrastructure services in emerging markets²⁰⁸ with the goal of preventing countries from defaulting to the DSR.

Extend the 'Total Package Approach' security assistance tools to digital connectivity solutions.

The DoD must extend its use of the 'total package approach,' in which training, technical assistance, initial support, software, and follow-on support are included,²⁰⁹ to its sale (or aid) of digital connectivity. The United States is a leader in exporting weapon systems specifically because of this approach. However, the CCP has copied the technique and sells "total tech packages," which locks out Western firms and US solutions.²¹⁰

Defend existing international norms in cyberspace and advance liberal democratic institutions to govern cyberspace.

The US must work with allies, leveraging initiatives such as the US Clean Network which mirrors the EU's 5G toolbox, to defend global digital norms, garner consensus for rules of the cyber road, establish rules of engagement for e-commerce and combating cybercrime. As 43 percent of countries did not legislate privacy or data protections as of 2020, US promotion of global standards

like the EU's General Data Protection Regulation (GDPR) would address a gap that China currently exploits.²¹¹

Provide legal and cyber aid to vulnerable states to expose Chinese debt trap and digital access schemes.

To date, many of the most unfavorable and questionable loans provided by the CCP or CCP-backed businesses target underdeveloped countries.^{212 213} Many of these governments do not have the expertise to assess Chinese contracts that require unfavorable debt repayment plans or life-cycle costs, which leaves the recipient government vulnerable to backdoors installed by China, allowing theft of data and intellectual property.^{214 215} US legal and cyber professionals can assist in shaping the decision-making process of these vulnerable governments targeted for BRI investment. They can shift the risk calculus by quantifying loss of data in comparison to benefits provided by DSR.

Conduct Integrated Deterrence

Chinese state-sponsored hackers are already infiltrating foreign systems to access proprietary and sensitive data with military and economic import.²¹⁶ DOD should adjust its deterrence strategy to encompass all capabilities of the full span of diplomatic, information, military, economic, financial, intelligence, and law enforcement (DIMEFIL) instruments of national power. A cyber-attack does not have to be met with a cyber response; the same applies to kinetic attacks and responses. Integrated deterrence involves the use of cyberspace and kinetic capabilities and other instruments of power to deter malicious cyberspace activity, as well as deter conventional kinetic operations.²¹⁷ Effective deterrence in cyberspace is achieved through continuous engagement with malicious actors who exploit current international norms. Cyber (deny) capabilities should be utilized below the level of armed conflict to prevent adversary attempts at influence operations, IP theft, election interference, as well as influence operations.²¹⁸

CONCLUSION

"The Full and unimpeded realization of China's DSR points to a world in which China wins conflicts without firing a shot."

Jonathan Hillman

The BRI challenge requires a sustained and coordinated 'whole of US' *and* allied and partner approach to prevent China from gaining advantage in the number (and depth) of 'friendly' countries across the globe, and to deny China the advantage in any potential conflict, militarily or economically. The advent of 6G interoperable technology, an increased focus on global governance, and the multiplicity of

investment funds available for domestic research and global development can position the United States to regain digital territory to ensure a free, open, and secure global internet.

Notes

-
1. General Paul M. Nakasone, “Posture statement of Gen. Paul M. Nakasone, commander, US Cyber Command before the 117th Congress,” April 5, 2022, <https://www.cybercom.mil/Media/News/Article/2989087/posture-statement-of-gen-paul-m-nakasone-commander-us-cyber-command-before-the/>.
 2. The White House, “National Cybersecurity Strategy,” March 2023, <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>.
 3. The White House, “National Cybersecurity Strategy.”
 4. Department of Defense Joint Staff, “Joint Publication 3-13, Information Operations,” November 20, 2014, I-2, https://irp.fas.org/doddir/dod/jp3_13.pdf.
 5. Catherine A. Theohary, “Information Warfare: Issues for Congress,” March 5, 2018, 5, <https://crsreports.congress.gov/product/pdf/R/R45142>.
 6. Theohary, “Information Warfare: Issues for Congress.”
 7. Brian Babcock-Lumish et al., “Managing the New Era of Deterrence and Warfare: Visualizing the Information Domain,” May 2023, 12, <https://www.understandingwar.org/backgrounder/managing-new-era-deterrence-and-warfare-visualizing-information-domain>.
 8. Lumish et al., “Managing the New Era of Deterrence and Warfare.”
 9. Theohary, “Information Warfare: Issues for Congress.”
 10. Lumish et al., “Managing the New Era of Deterrence and Warfare,” 11.
 11. Philip M Seib, *Information at War: Journalism, Disinformation, and Modern Warfare* (Cambridge, Uk; Medford, Ma: Polity Press, 2021).
 12. “Report Reveals 65% of Cyberattacks Targeted at U.S. | Security Magazine,” www.securitymagazine.com, April 26, 2023, <https://www.securitymagazine.com/articles/99257-report-reveals-65-of-cyberattacks-targeted-at-us>.
 13. “MAP | Kaspersky Cyberthreat Real-Time Map,” MAP | Kaspersky Cyberthreat real-time map, 2018, accessed May 18, 2023, <https://cybermap.kaspersky.com/>.
 14. “Foreign Influence Operations and Disinformation | Cybersecurity and Infrastructure Security Agency CISA,” www.cisa.gov, n.d., accessed May 7, 2023, <https://www.cisa.gov/topics/election-security/foreign-influence-operations-and-disinformation>.

-
15. Peter Bell, "Public Trust in Government: 1958-2022," Pew Research Center - U.S. Politics & Policy, June 6, 2022, <https://www.pewresearch.org/politics/2022/06/06/public-trust-in-government-1958-2022/>.
 16. The White House, "The National Strategy to Secure Cyberspace" (Washington, D.C.: The White House, February 2003), <https://www.hsdl.org/c/view?docid=1040>.
 17. The White House, "The National Strategy to Secure Cyberspace."
 18. Department of Homeland Security, "Creation of the Department of Homeland Security," Department of Homeland Security, September 24, 2015, <https://www.dhs.gov/creation-department-homeland-security>.
 19. The White House, "The National Strategy to Secure Cyberspace," 49–52.
 20. The White House, "The National Strategy to Secure Cyberspace," 37–42.
 21. "The Administration Unveils Its Cybersecurity Legislative Proposal," Whitehouse.Gov, May 12, 2011, <https://obamawhitehouse.archives.gov/blog/2011/05/12/administration-unveils-its-cybersecurity-legislative-proposal>.
 22. United States Cyber Command, "Command History," Cybercom.mil, 2017, accessed April 29, 2023, <https://www.cybercom.mil/About/History/>.
 23. United States Cyber Command, "Command History."
 24. Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," 2011, <https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf>.
 25. Daniel Moore, *Offensive Cyber Operations - Understanding Intangible Warfare* (Oxford University Press, 2022), 122, <https://global.oup.com/academic/product/offensive-cyber-operations-9780197657553?cc=us&lang=en&>.
 26. Moore, *Offensive Cyber Operations*, 123.
 27. Moore, *Offensive Cyber Operations*, 123.
 28. Erica D Lonergan and Jacquelyn Schneider, "The Power of Beliefs in U.S. Cyber Strategy: The Evolving Role of Deterrence, Norms, and Escalation," *Journal of Cybersecurity* 9, no. 1 (January 1, 2023): 4, <https://doi.org/10.1093/cybsec/tyad006>.
 29. "The DoD Cyber Strategy," April 2015, 9.

30. Federal Register, “Cybersecurity Act of 2015,” Pub. L. No. PL 114-113, Division N, <https://www.federalregister.gov/documents/2016/06/15/2016-13742/cybersecurity-information-sharing-act-of-2015-final-guidance-documents-notice-of-availability>.

31. Dustin Volz, “Trump, Seeking to Relax Rules on U.S. Cyberattacks, Reverses Obama Directive,” *Wall Street Journal*, August 16, 2018, sec. Politics, <https://www.wsj.com/articles/trump-seeking-to-relax-rules-on-u-s-cyberattacks-reverses-obama-directive-1534378721>.

32. Volz, “Trump, Seeking to Relax Rules.”

33. The White House, “National Cyber Strategy,” September 2018, <https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>.

34. The White House, “National Cyber Strategy, 2018,” 1–7.

35. Department of Defense, “Summary, Department of Defense Cyber Strategy, 2018,” 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

36. “Summary, Department of Defense Cyber Strategy 2018,” 2.

37. “Summary, Department of Defense Cyber Strategy 2018,” 5–6.

38. The White House, “National Cybersecurity Strategy,” March 2023, <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>.

39. Kaju, “How To Crush Your Enemies: Facebook vs Friendster,” *My Affiliate Rockstar Child* (blog), July 11, 2019, <https://myaffiliaterockstar.talkingtaiwan.com/how-to-crush-your-enemies-facebook-vs-friendster/>.

40. “Twitter | Company, History, Description, Elon Musk, & Uses | Britannica,” April 21, 2023, <https://www.britannica.com/topic/Twitter>.

41. Hammaad Salik and Zaheema Iqbal, “Social Media and National Security,” *The Geopolitics*, September 10, 2019, <https://thegeopolitics.com/social-media-and-national-security/>.

42. Statista, “U.S. Number of Social Media Users 2023 | Statista,” Statista (Statista, 2017), <https://www.statista.com/statistics/278409/number-of-social-network-users-in-the-united-states/>.

43. Jason A. Gallo and Clare Y. Cho, “Social Media: Misinformation and Content Moderation Issues for Congress,” January 27, 2021, <https://crsreports.congress.gov/product/pdf/R/R46662>.

-
44. Gallo and Cho, "Social Media: Misinformation."
45. Samantha Korta, "Fake News, Conspiracy Theories, and Lies: An Information Laundering Model for Homeland Security," *Homeland Security Affairs* (March 2018): 80, <https://www.proquest.com/scholarly-journals/fake-news-conspiracy-theories-lies-information/docview/2206253872/se-2>.
46. Cindy Otis, "The Mainstreaming of Conspiracy Theories," interview by Darragh Worland, *Is That A Fact*, News Literacy Project, audio transcript, <https://newslit.org/podcast/the-mainstreaming-of-conspiracy-theories/>.
47. Dina ElBoghdady, "Market Quavers after Fake AP Tweet Says Obama Was Hurt in White House Explosions," *Washington Post*, April 23, 2013, sec. Business, https://www.washingtonpost.com/business/economy/market-quavers-after-fake-ap-tweet-says-obama-was-hurt-in-white-house-explosions/2013/04/23/d96d2dc6-ac4d-11e2-a8b9-2a63d75b5459_story.html.
48. Salik and Iqbal, "Social Media and National Security."
49. Cloudflare, "What Is a Bot? | Bot Definition | Cloudflare," *Cloudflare*, n.d., accessed April 23, 2023, <https://www.cloudflare.com/learning/bots/what-is-a-bot/>.
50. Cloudflare, "What Is a Social Media Bot? | Social Media Bot Definition | Cloudflare," *Cloudflare*, accessed April 25, 2023, <https://www.cloudflare.com/learning/bots/what-is-a-social-media-bot/>.
51. Cloudflare, "What is a Social Media Bot?"
52. Cloudflare, "What is a Social Media Bot?"
53. Samantha Murphy Kelly, "Snapchat's New AI Chatbot Is Already Raising Alarms among Teens and Parents | CNN Business," *CNN*, April 27, 2023, <https://www.cnn.com/2023/04/27/tech/snapchat-my-ai-concerns-wellness/index.html>.
54. Kelly, "Snapchat's New AI Chatbot."
55. Emerson T Brooking and P W Singer, "How Twitter Is Changing Modern Warfare," *The Atlantic* (The Atlantic, October 11, 2016), <https://www.theatlantic.com/magazine/archive/2016/11/war-goes-viral/501125/>.
56. Scott Jasper, *Russian Cyber Operations: Coding the Boundaries of Conflict* (Georgetown University Press, 2020) p 74.
57. Nicu Popescu and Stanislav Secieru, "Hacks, Leaks and Disruptions – Russian Cyber Strategies | European Union Institute for Security Studies," *Europa.eu*, October 23, 2018,

<https://www.iss.europa.eu/content/hacks-leaks-and-disruptions-%E2%80%93-russian-cyber->

strategies.

58. Andrew S. Bowen, “Russian Cyber Units,” Congressional Research Service, February 2, 2022, <https://crsreports.congress.gov/product/pdf/IF/IF11718>.

59. Neil MacFarquhar, “A Powerful Russian Weapon: The Spread of False Stories,” *The New York Times*, August 28, 2016, sec. World, <http://www.nytimes.com/2016/08/29/world/europe/russia-sweden-disinformation.html>.

60. Peter Pomerantsev and Michael Weiss, “The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money a Special Report Presented by the Interpreter, a Project of the Institute of Modern Russia” (Institute of Modern Russia, 2014), https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev_The_Menace_of_Unreality.pdf.

61. James Andrew Lewis, “‘Compelling Opponents to Our Will’: The Role of Cyber Warfare in Ukraine,” 2015, NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/uploads/2018/10/Ch04_CyberWarinPerspective_Lewis.pdf.

62. Jessikka Aro, “The Cyberspace War: Propaganda and Trolling as Warfare Tools,” *European View* 15, no. 1 (June 2016): 121–32, <https://doi.org/10.1007/s12290-016-0395-5>.

63. Jasper, *Russian Cyber Operations*, p 35.

64. Lloyd J. Austin III, “2022 National Defense Strategy” (Secretary of Defense, October 27, 2022) 6, <https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF>.

65. Aro, “The Cyberspace War: Propaganda and Trolling.”

66. Edward Lucas and Ben Nimmo, “CEPA INFOWAR PAPER No 1, Information Warfare: What Is It and How to Win It?,” November 2015, 3, Center for European Policy Analysis, <https://www.yumpu.com/en/document/view/55861600/cepa-infowar-paper-no-1>.

67. James R. Van de Velde, Ph.D., Professor, “IS-19 lecture,” ES-6710, OIE Industry Study, Eisenhower School, National Defense University April 27, 2023.

68. Van de Velde, April 27, 2023.

69. Jasper, *Russian Cyber Operations*, p 79.

70. “Unclassified Posture Statement of General Paul M. Nakasone Commander, United States Cyber Command before the 118TH Congress Senate Committee on Armed Services,” March 7, 2023, <https://www.armed-services.senate.gov/imo/media/doc/CDRUSCYBERCOM%20SASC%20Posture%20Statement%20FINAL%20.pdf>.

-
71. Nakasone, "Unclassified Posture Statement."
72. Christine Rosen, "Misinformed about Disinformation," *National Review*, January 19, 2023, <https://www.nationalreview.com/magazine/2023/02/06/misinformed-about-disinformation/>.
73. Eddie Scarry, "Russia's memes had no quantifiable effect on our elections, but we have to keep hearing about it anyway," *Washington Examiner*, December 18, 2018. Quoted in "Russian Memes Have No Effect Because They Echo Existing Political Sentiments," *Gale Opposing Viewpoints Online Collection*, Farmington Hills, MI: Gale, 2023. *Gale In Context: Global Issues* (accessed March 20, 2023), <https://link-gale-com.nduezproxy.idm.oclc.org/apps/doc/APIFJI290471003/GIC?u=wash60683&sid=bookmark-GIC&xid=d29cac32>.
74. Carla Norris, "A Book Review: *Information at War, Journalism, Disinformation, and Modern Warfare* by Philip Seib" (March 5, 2023).
75. Bowen, "Russian Cyber Units."
76. Lt Col Jarred Prier, "Commanding the Trend: Social Media as Information Warfare," *Strategic Studies Quarterly*, Vol. 11, no. 4 (Winter 2017): 50–85, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-11_Issue-4/Prier.pdf.
77. Anya Schiffrin, "Journal of International Affairs Editorial Board Disinformation and Democracy: The Internet Transformed Protest but Did Not Improve Democracy," *Source: Journal of International Affairs* 71, no. 1 (2017): 117–126, <https://www.proquest.com/docview/2054916939>.
78. OECD, "Disinformation and Russia's War of Aggression against Ukraine," OECD, November 3, 2022, <https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/>.
79. Prier, "Commanding the Trend: Social Media as Information Warfare."
80. Prier, "Commanding the Trend: Social Media as Information Warfare."
81. "2020 National Election Controversies," Gale.com (Gale, part of Cengage Group, 2021), <https://link.gale.com/apps/doc/DZYIXG049385636/GIC?u=wash60683&sid=bookmark-GIC&xid=809105f8>.
82. OECD, Disinformation and Russia's War of Aggression against Ukraine.
83. Elizabeth Gehrman, "The Isolation of Social Media," *hms.harvard.edu* (Harvard Medicine, The Magazine of Harvard Medical School, Spring 2022), <https://hms.harvard.edu/magazine/viral-world/isolation-social-media>.

84. “Digital Media Literacy: How Filter Bubbles Isolate You,” GCFGlobal.org, n.d., <https://edu.gcfglobal.org/en/digital-media-literacy/how-filter-bubbles-isolate-you/1/#>.

85. Nakasone, “Unclassified Posture Statement.”

86. Nakasone, “Unclassified Posture Statement.”

87. CISA, “CISA, Cyber National Mission Force Leaders Share How They Partner: First-Ever Ops Revealed to Industry | CISA,” [www.cisa.gov](https://www.cisa.gov/news-events/news/cisa-cyber-national-mission-force-leaders-share-how-they-partner-first-ever-ops-revealed-industry#:~:text=The%20CNMF%20mission%20is%20broad), April 25, 2023, <https://www.cisa.gov/news-events/news/cisa-cyber-national-mission-force-leaders-share-how-they-partner-first-ever-ops-revealed-industry#:~:text=The%20CNMF%20mission%20is%20broad>.

88. Bohdan Harasymiw, “Confronting Russian Disinformation in Ukraine: A Tangled Skein,” *Seton Hall Journal of Diplomacy and International Relations*, 22, no. 1 (Spring/Summer 2021): 47-59, <https://web.p.ebscohost.com/abstract?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=15386589&AN=157720275&h=dcqWabEOe2QIBxttI9s%2b%2fbKdS8iB%2fz7%2bp30i18y10jiCYHczjThYqY3vsPQeASSyk%2brewfbU%2bKI3hW3rgbakjA%3d%3d&crl=c&resultNs=AdminWebAuth&resultLocal=ErrCrlNotAuth&crlhashurl=login.aspx%3fdirect%3dtrue%26profile%3dehost%26scope%3dsite%26authtype%3dcrawler%26jrnl%3d15386589%26AN%3d157720275>.

89. Harasymiw, *Confronting Russian Disinformation in Ukraine*.

90. OECD, *Disinformation and Russia’s War of Aggression against Ukraine*.

91. Lucas and Nimmo, “CEPA INFOWAR PAPER No. 1,” 3.

92. Brandy Zadrozny et al., “Congress Releases 3,000 Russian Ads — Including Some That Targeted Fans of Fox News,” NBC News, May 11, 2018, <https://www.nbcnews.com/tech/tech-news/sean-hannity-black-lives-matter-among-targets-russian-influence-campaign-n872926>.

93. Lucas and Nimmo, “CEPA INFOWAR PAPER No. 1,” 7.

94. Global Engagement Center, “GEC Special Report: Pillars of Russia’s Disinformation and Propaganda Ecosystem,” US Department of State, August 2020, https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf.

95. Lucas and Nimmo, “CEPA INFOWAR PAPER No. 1,” p 5.

96. Michael J Mazarr et al., “Hostile Social Manipulation: Present Realities and Emerging Trends,” Rand.org (RAND Corporation, 2019),

https://www.rand.org/pubs/research_reports/RR2713.html.

97. Mazarr et al., Hostile Social Manipulation.

98. Cyberspace Solarium Commission. "March 2020 CSC Report" March 11, 2020. <https://cybersolarium.org/march-2020-csc-report/march-2020-csc-report/>.

99. Rain Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective," Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, October 2018, https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf.

100. Ellen Nakashima, "Russian Military Was behind 'NotPetya' Cyberattack in Ukraine, CIA Concludes," *The Washington Post*, January 12, 2018, https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html.

101. Josephine Wolff, "How the NotPetya Attack Is Reshaping Cyber Insurance," Tech Stream, Brookings, December 1, 2021, <https://www.brookings.edu/techstream/how-the-notpetya-attack-is-reshaping-cyber-insurance/>.

102. Rob Sloan, "A Perspective on Russian Cyberattacks and Disinformation," *Wall Street Journal Pro Cybersecurity*, June 21, 2022, <https://www.wsj.com/articles/a-perspective-on-russian-cyberattacks-and-disinformation-11655845822>.

103. Craig Timberg, "7 Takeaways from the Vulkan Files Investigation," *Washington Post*, March 30, 2023, <https://www.washingtonpost.com/national-security/2023/03/30/takeaways-vulkan-files-investigation/>.

104. Dr. Christopher Whyte, "NTC Vulkan Leak Shows Evolving Russian Cyberwar Capabilities," CSO Online, April 7, 2023, <https://www.csoonline.com/article/3692821/ntc-vulkan-leak-shows-evolving-russian-cyberwar-capabilities.html>.

105. Eric Tucker Press The Associated, "US Busts Russian Cyber Operation in Dozens of Countries," *Military Times*, May 9, 2023, <https://www.militarytimes.com/news/your-military/2023/05/09/us-busts-russian-cyber-operation-in-dozens-of-countries/>.

106. Andrei Soldatov and Irina Borogan, "Russian Cyberwarfare: Unpacking the Kremlin's Capabilities," CEPA, September 8, 2022, <https://cepa.org/comprehensive-reports/russian-cyberwarfare-unpacking-the-kremlins-capabilities/>.

107. Soldatov and Borogan, "Russian Cyberwarfare: Unpacking the Kremlin's Capabilities."

108. Joshua Kurlantzick, “China’s Growing Attempts to Influence U.S. Politics,” Council on Foreign Relations, October 31, 2022, <https://www.cfr.org/article/chinas-growing-attempts-influence-us-politics>.

109. Krassi Twigg and Kerry Allen, “The Disinformation Tactics Used by China,” *BBC News*, March 12, 2021, sec. Reality Check, <https://www.bbc.com/news/56364952>.

110. Jonathan Landay and Yew Lun Tian, “U.S. Counterintelligence Warns of China Stepping up Influence Operations,” *Reuters*, July 7, 2022, sec. United States, <https://www.reuters.com/world/us/us-counterintelligence-warns-china-stepping-up-influence-operations-2022-07-06/>.

111. James Tager, “Made in Hollywood, Censored by Beijing,” PEN America, August 5, 2020, 23, <https://pen.org/report/made-in-hollywood-censored-by-beijing/>.

112. Christopher Balding, “China’s Collection of Data on Foreigners Is a National Security Risk,” *Discourse*, November 29, 2021, <https://www.discoursemagazine.com/politics/2021/11/29/chinas-collection-of-data-on-foreigners-is-a-national-security-risk/>.

113. Uneeb Asim, “The Great Firewall of China. Everything You Need to Know - Techs Motion,” *www.techsmotion.com*, June 5, 2022, <https://www.techsmotion.com/great-firewall-of-china/>.

114. Adam Segal et al., “Roundtable: The Future of Cybersecurity across the Asia-Pacific,” April 2020, https://www.nbr.org/wp-content/uploads/pdfs/publications/ap15-2_cyberrrt_apr2020.pdf.

115. Sarah Fitzpatrick and Kit Ramgopal, “Hackers Linked to Chinese Government Stole Millions in Covid Benefits,” *NBC News*, December 5, 2022, <https://www.nbcnews.com/tech/security/chinese-hackers-covid-fraud-millions-rcna59636>.

116. Nalani Fraser et al., “APT41: A Dual Espionage and Cyber Crime Operation,” *Mandiant*, August 7, 2019, <https://www.mandiant.com/resources/blog/apt41-dual-espionage-and-cyber-crime-operation>.

117. Kenton Thibaut, “Chinese Discourse Power: Ambitions and Reality in the Digital Domain,” *Atlantic Council*, August 24, 2022, 10, <https://www.atlanticcouncil.org/in-depth-research-reports/report/chinese-discourse-power-ambitions-and-reality-in-the-digital-domain/>.

118. Nathan Beauchamp-Mustafaga and Michael S. Chase, “Borrowing a Boat out to Sea | Beauchamp-Mustafaga and Chase” (Johns Hopkins School of Advanced International Studies, Foreign Policy Institute, 2019), 15, <https://www.fpi.sais-jhu.edu/borrowing-a-boat-out-to-sea-pdf>. *See also* Renee DiResta et al., “Telling China’s Story: The Chinese Communist Party’s Campaign to Shape Global Narratives,” *Fsi.stanford.edu*, July 20, 2020, <https://fsi.stanford.edu/publication/telling-chinas-story>.

-
119. Beauchamp-Mustafaga and Chase, *Borrowing a Boat*, 9.
120. Beauchamp-Mustafaga and Chase, *Borrowing a Boat*, v.
121. Thibaut, “Chinese Discourse Power,” 7.
122. DiResta et al, *Telling China's Story*, 7.
123. Fergus Ryan et al., “#StopXinjiang Rumors: The CCP’s decentralised disinformation campaign,” (Barton, Australia: Australian Strategic Policy Institute, December 2, 2021), 6, <https://www.aspi.org.au/report/stop-xinjiang-rumors/>.
124. Beauchamp-Mustafaga and Chase, *Borrowing a Boat*, 94. See also DiResta et al, *Telling China's Story*, 15.
125. DiResta et al, *Telling China's Story*, 20.
126. DiResta et al, *Telling China's Story*, 25
127. DiResta et al, *Telling China's Story*, 25
128. Jeff Kao and Mia Shuang Li, “How China Built a Twitter Propaganda Machine Then Let It Loose on Coronavirus,” *ProPublica*, March 26, 2020, <https://www.propublica.org/article/how-china-built-a-twitter-propaganda-machine-then-let-it-loose-on-coronavirus>.
129. Jeff Kao et al, “How China Spreads Its Propaganda Version of Life for Uyghurs,” *ProPublica* and *New York Times*, June 23, 2021, <https://www.propublica.org/article/how-china-uses-youtube-and-twitter-to-spread-its-propaganda-version-of-life-for-uyghurs-in-xinjiang>.
130. The White House, “National Cybersecurity Strategy,” 3.
131. Segal et al., “Roundtable: The Future of Cybersecurity across the Asia-Pacific.”
132. Greg Austin, “Evaluating China’s Cyber Power,” *thediplomat.com*, October 26, 2016, <https://thediplomat.com/2016/10/evaluating-chinas-cyber-power>.
133. Mikk Raud , “China and Cyber: Attitude, Strategies and Organisation, ” NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), Tallinn 2016, https://ccdcoe.org/uploads/2018/10/CS_organisation_CHINA_092016_FINAL.pdf.
134. “Section 2: China’s Cyber Capabilities: Warfare, Espionage, and Implications for the United States,” U.S.-China Economic & Security Review Commission, https://www.uscc.gov/sites/default/files/2022-11/Chapter_3_Section_2--Chinas_Cyber_Capabilities.pdf.

135. Raud, “China and Cyber.”

136. Christopher Wray, “The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States” (Hudson Institute, Video Event: China’s Attempt to Influence U.S. Institutions, July 7, 2020), <https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states>.

137. Wray, “The Threat Posed by the Chinese.”

138. United States–China Economic and Security Commission, “China’s Cyber Capabilities: Warfare, Espionage, and Implications for the United States,” https://www.uscc.gov/sites/default/files/2022-11/Chapter_3_Section_2--Chinas_Cyber_Capabilities.pdf.

139. Derek B. Johnson, “How China Uses Cyber Theft and Information Warfare,” FCW, May 6, 2019, <https://fcw.com/security/2019/05/how-china-uses-cyber-theft-and-information-warfare/256198/>.

140. Raashi Shah Assistant Manager et al., “Global Research and Analytics Firm,” www.aranca.com, September 9, 2020, <https://www.aranca.com/knowledge-library/articles/investment-research/ip-theft-china-and-beyond>. (Figure 14).

141. Commission on the Theft of American Intellectual Property. “The I.P. Commission Report 2017 Update.” Feb 23, 2017. <https://www.nbr.org/publication/update-to-the-ip-commission-report-february-2017/>.

142. Simon Handler, “The 5×5—China’s Cyber Operations,” *Atlantic Council*, January 30, 2023, <https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-chinas-cyber-operations/>.

143. Yossi, “U.S. Accuses China of Cyber-Spying - Hamodia.com,” Hamodia, May 20, 2014, <https://hamodia.com/2014/05/19/u-s-accuses-china-cyber-spying/>. (Figure 15).

144. Commission on the Theft of American Intellectual Property. “The I.P. Commission Report.”

145. DiResta et al, Telling China’s Story, 7.

146. Lili Pike, “How China Uses Global Media to Spread Its Views — and Misinformation,” Nieman Lab, May 18, 2022, 2, <https://www.niemanlab.org/reading/how-china-uses-global-media-to-spread-its-views-and-misinformation/>.

147. DiResta et al, Telling China’s Story, 41.

148. “APT43: North Korean Group Uses Cybercrime to Fund Espionage Operations,” Mandiant, accessed April 30, 2023, <https://www.mandiant.com/resources/reports/apt43-north-korea-cybercrime-espionage>.

149. Tae-jun Kang, "North Korea's Influence Operations Revealed," *The Diplomat*, July 25, 2018, <https://thediplomat.com/2018/07/north-koreas-influence-operations-revealed>.

150. Jessica Guynn, "Facebook information warfare: Inside Iran's shadowy operations to target you on social media," *USA Today*, January 10, 2020, <https://www.usatoday.com/story/tech/2020/01/10/iran-influence-operations-target-americans-after-soleimani-killing/4422491002/>.

151. "6 U.S.C. § 1500 (2021), 'National Cyber Director' ," uscode.house.gov, accessed April 17, 2023, <https://uscode.house.gov/view.xhtml?hl=false&edition=prelim&path=%2Fprelim%40title6%2Fchapter6%2Fsubchapter1&req=granuleid%3AUSC-2021-title6-chapter6-subchapter1&num=0>.

152. 6 U.S.C. § 1500 (2021), "National Cyber Director."

153. The White House, "National Cyber Strategy, 2018."

154. The White House, "National Cyber Strategy, 2018."

155. 6 U.S.C. § 1500 (2021), "National Cyber Director."

156. 6 U.S.C. § 1500 (2021), "National Cyber Director."

157. Theohary, "Information Warfare: Issues for Congress."

158. 6 U.S.C. § 1500 (2021), "National Cyber Director."

159. Mr. Mohamed Telab, Deputy Regional Director, Region 2: NY, NJ, PR and USVI, Cybersecurity and Infrastructure Security Agency (CISA), "CISA Overview," face-to-face, Brief to Eisenhower School Seminar on Operations in the Information Environment, March 3, 2023.

160. "Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) | CISA," Cybersecurity and Infrastructure Security Agency CISA, n.d., <https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia#:~:text=Cyber%20Incident%20Reporting%20Requirements%3A%20CIRCIA>.

161. "National Council of ISACs," [natlcouncilofisacs](https://www.nationalisacs.org/), <https://www.nationalisacs.org/>.

162. "California Civil Code §1798.82," [leginfo.legislature.ca.gov](https://leginfo.ca.gov), accessed May 16, 2023, https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.82&lawCode=CIV.

163. D Mulligan and K Bamberger, “HomeSecurity Breach Notification Laws: Views

from Chief Security Officers, Samuelson Law, Technology & Public Policy Clinic, University of California-Berkeley School of Law.,” Berkeley Law, 2007, <http://www.law.berkeley.edu/>.

164. “Rebooting Letters of Marque for Private Sector, Active Cyber Defense – CSIAC.”

165. “Bug Bounty List - All Active Programs in 2020,” Bugcrowd, accessed May 17, 2023, <https://www.bugcrowd.com/bug-bounty-list/>.

166. “Bill Text - SB-1001 Bots: Disclosure.,” [leginfo.legislature.ca.gov](https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1001), September 28, 2018, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1001.

167. Robert Bateman, “How to Comply with California’s Bot Disclosure Law,” Terms Feed, February 18, 2023, <https://www.termsfeed.com/blog/ca-bot-disclosure-law/>.

168. Bateman, How to Comply with California’s Bot Disclosure Law.

169. The Office of U.S. Senator for Hawaii, Brian Schatz, “Schatz, Cotton, Murphy, Britt Introduce Bipartisan Legislation to Help Protect Kids from Harmful Impacts of Social Media | U.S. Senator Brian Schatz of Hawaii,” [www.schatz.senate.gov](https://www.schatz.senate.gov/news/press-releases/schatz-cotton-murphy-britt-introduce-bipartisan-legislation-to-help-protect-kids-from-harmful-impacts-of-social-media), April 26, 2023, <https://www.schatz.senate.gov/news/press-releases/schatz-cotton-murphy-britt-introduce-bipartisan-legislation-to-help-protect-kids-from-harmful-impacts-of-social-media>.

170. “United States Pay Television Content Advisory System,” Wikipedia, April 6, 2023, https://en.wikipedia.org/wiki/United_States_pay_television_content_advisory_system.

171. Michael P. Fischerkell et al, “Deterrence Is Not a Credible Strategy for Cyberspace (and What Is),” WELCH AWARD 2018 (Institute for Defense Analyses, 2019), 7, <http://www.jstor.org/stable/resrep22904.3>.

172. Moore, *Offensive Cyber Operations - Understanding Intangible Warfare*, 127.

173. Fischerkell, Harknett, and Analyses, “Deterrence Is Not a Credible Strategy for Cyberspace (and What Is),” 8.

174. “Cybersecurity Supply and Demand Heat Map,” Cyberseek.org, 2017, accessed April 28, 2023, <https://www.cyberseek.org/heatmap.html>.

175. “Cybersecurity Supply/Demand Heat Map.”

176. Chiradeep BasuMallick, “Top 10 Cybersecurity Colleges in the US in 2022,” Spiceworks IT Careers and Skills, December 23, 2022, <https://www.spiceworks.com/tech/it-careers-skills/articles/best-cybersecurity-colleges/>.

177. Statista Research Department, “Share of households with internet access in Finland from 2009 to 2022,” [statista](https://www.statista.com/statistics/377766/household-internet-access-in-finland/), March 14, 2023, <https://www.statista.com/statistics/377766/household-internet-access-in-finland/>.

-
178. Statista Research Department, “Share of households with internet.”
179. Office of Educational Technology, “Advancing Digital Equity for All: Community-Based Recommendations for Developing Effective Digital Equity Plans to Close the Digital Divide and Enable Technology-Empowered Learning,” US Department of Education, September 2022, https://tech.ed.gov/files/2022/09/DEER-Resource-Guide_FINAL.pdf.
180. Eva Toome, “Cyber Security Education in Estonia: From Kindergarten to NATO Cyber Defence Centre,” Education Estonia, March 30, 2022, <https://www.educationestonia.org/cyber-security-education-in-estonia/>.
181. American Search Engine Employee, interview by OIE Industry Study, California, April 12, 2023.
182. American Search Engine Employee, interview by OIE Industry Study, California, April 12, 2023.
183. Cybersecurity Expert from Leading US Technology Firm, interview by OIE Industry Study, California, April 12, 2023.
184. Richard Ghiasy and Rajeshwari Krishnamurthy, “China’s Digital Silk Road and the Global Digital Order,” *The Diplomat*, April 12, 2021, <https://thediplomat.com/2021/04/chinas-digital-silk-road-and-the-global-digital-order/>.
185. Ghiasy and Krishnamurthy, “China's Digital Silk Road.”
186. Jared Cohen and Richard Fontaine. "Uniting the Techno- Democracies." Foreign Affairs, Nov 2020, 112-122, <https://www.proquest.com/magazines/uniting-techno-democracies/docview/2452331710/se-2>.
187. Lili Pike, “How China Uses Global Media to Spread Its Views—and Misinformation,” *Grid News*, May 18, 2022.
188. Sarah Sewall, Tyler Vandenberg, and kaj Malden, “China’s BeiDou: New Dimensions of Great Power Competition,” *Harvard Kennedy School: Belfer Center*, February 2023, 12, https://www.belfercenter.org/sites/default/files/files/publication/Chinas-BeiDou_V10.pdf.
189. Rumi Aoyama. "China’s Dichotomous BeiDou Strategy: Led by the Party for National Deployment, Driven by the Market for Global Reach." *The Journal of Contemporary East Asia Studies* 11, no. 2 (12 2022): 282-299, doi:<https://doi.org/10.1080/24761028.2023.2178271>.

190. Namrata Goswami. "The Economic and Military Impact of China's BeiDou Navigation System." *The Diplomat*, July 01, 2020, <https://thediplomat.com/2020/07/the-economic-and-military-impact-of-chinas-beidou-navigation-system/>.

191. David H. Millner, Stephen Maksim, and Marissa Huhmann. "BeiDou China's GPS Challenger Takes its Place on the World Stage." *Joint Force Quarterly: JFQ* no. 105 (Second, 2022): 23-31, <https://www.proquest.com/trade-journals/beidou-chinas-gps-challenger-takes-place-on-world/docview/2660147778/se-2>.

192. John Xie, "China's Rival GPS Navigation Carries Big Risks," *Voice of America*, https://www.voanews.com/a/east-asia-pacific_voa-news-china_chinas-rival-gps-navigation-carries-big-risks/6192460.html (accessed May 15, 2023).

193. Lili Yulyadi Arnakim, Moch Faisal Karim, and Bernadetta Nindya Kusuma Pradipta, "Implications of China's Digital Silk Road for US Domination of the International System." *Contemporary Chinese Political Economy and Strategic Relations* 7, no. 1 (04, 2021): 79-105, VI,X,XIII, <https://www.proquest.com/scholarly-journals/implications-chinas-digital-silk-road-us/docview/2578204500/se-2>.

194. Meia Nouwens, Camille Lons, Nawafel Shehab, Scott Malcomson, and Alexander Neill, "China's Digital Silk Road: Integration into National IT Infrastructure and Wider Implications for Western Defence Industries," *International Institute for Strategic Studies*, 2021, 1-58, <https://www.iiss.org/blogs/research-paper/2021/02/china-digital-silk-road-implications-for-defence-industry>.

195. Didi Kirsten Tatlow, "China Targets Israeli Technology in Quest for Global Dominance as US Frets," *Newsweek*, August 10, 2022, <https://www.newsweek.com/2022/08/19/china-targets-israeli-technology-quest-global-dominance-us-frets-1727108.html>.

196. Adam Segal and Gordon M. Goldstein, "Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet," *The Council for Foreign Relations*, Last modified July 2022, <https://www.cfr.org/report/confronting-reality-in-cyberspace/introduction>.

197. ITU News. "ITU: Top Contributors to ICT Growth in China." *ITU News*, August 11, 2022, <https://www.itu.int/hub/2022/08/itu-top-contributors-china/>.

198. ITU News.

199. Omri Wallach, "The history of the gaming industry in one chart," *World Economic Forum*, November 27, 2020, <https://www.weforum.org/agenda/2020/11/gaming-games-consels-xbox-play-station-fun/>.

200. Charity Wright. "China's Digital Colonialism: Espionage and Repression Along the Digital Silk Road." *The SAIS Review of International Affairs* 41, no. 2 (2021), 96, 98.

201. Esa Makinen, “Truth About the War,” *HS: Ytimessa*, May 05, 2023, Secret room inside popular game contains independent journalism forbidden in Russia | HS.fi.

202. Sarah Sewall, Tyler Vandenberg, and kaj Malden, “China’s BeiDou: New Dimensions of Great Power Competition,” *Harvard Kennedy School: Belfer Center*, February 2023, 13, https://www.belfercenter.org/sites/default/files/files/publication/Chinas-BeiDou_V10.pdf.

203. Sarah Sewall, Tyler Vandenberg, and kaj Malden, “China’s BeiDou: New Dimensions of Great Power Competition,” *Harvard Kennedy School: Belfer Center*, February 2023, 14, https://www.belfercenter.org/sites/default/files/files/publication/Chinas-BeiDou_V10.pdf.

204. Shubhangi Kharche and Prajakta Dere, “Interoperability Issues and Challenges in 6G Networks,” *Journal of Mobile Multimedia*, April 4, 2022, 1445–70, <https://doi.org/10.13052/jmm1550-4646.1856>.

205. Richard Ghiasy and Rajeshwari Krishnamurthy, “China’s Digital Silk Road and the Global Digital Order,” *The Diplomat*, April 12, 2021. <https://thediplomat.com/2021/04/chinas-digital-silk-road-and-the-global-digital-order/>.

206. Elisabeth Braw, “The 6G Showdown with China Is Coming,” *Financial Times*, November 30, 2022, sec. Technology sector, <https://www.ft.com/content/4a1eaf64-c956-45ab-9473-d1437e36d3a4>.

207. Daniel F. Runde and Sundar R. Ramanujam, “Digital Governance: It Is Time for the United States to Lead Again,” *CSIS*, August 02, 2021, <https://www.csis.org/analysis/digital-governance-it-time-united-states-lead-again>.

208. USAID, “Digital Invest,” <https://www.usaid.gov/digital-development/digital-invest#:~:text=Digital%20Invest%20is%20a%20blended,digital%20ecosystems%20in%20emerging%20markets>.

209. Department of Defense, Defense Security Cooperation Agency, Security Assistance Management Manual (SAMM), Chapter 4, C4.3.2, “Total Package Approach,” <https://samm.dsca.mil/chapter/chapter-4>.

210. Jennifer Hillman and David Sacks. Rep. *China’s Belt and Road: Implications for the United States*. Council on Foreign Relations, 2021, <https://www.cfr.org/report/chinas-belt-and-road-implications-for-the-united-states/findings>.

211. Charity Wright, “China’s Digital Colonialism: Espionage and Repression Along the Digital Silk Road.” *The SAIS Review of International Affairs*, 41, no. 2 (2021), 94.

212. Balazs ujvari, “The Belt and Road Initiative – the ASEAN perspective,” *Egmont Institute*, 2019, *The Belt and Road Initiative — the ASEAN Perspective on JSTOR*.

213. Pearl Risberg, “The Give-and-Take of BRI in Africa.” *Center for Strategic & International Studies*, April 08, 2019, accessed November 02, 2022, The Give-and-Take of BRI in Africa | Center for Strategic and International Studies (csis.org).

214. Daniel Lindley, “Assessing China’s Motives: How the Belt and Road Initiative Threatens US Interests.” *Journal of Indo-Pacific Affairs*, Air University Press, August 01, 2022, accessed September 30, 2022, Assessing China’s Motives: How the Belt and Road Initiative Threatens US Interests > Air University (AU) > Journal of Indo-Pacific Affairs Article Display.

215. Charity Wright, “China’s Digital Colonialism: Espionage and Repression Along the Digital Silk Road.” *The SAIS Review of International Affairs* 41, no. 2 (2021), 70, 94.

216. Wright, “China’s Digital Colonialism.”

217. James Van de Velde, “Cyber Deterrence Is Dead!”⁴⁴.

218. Van de Velde, “Cyber Deterrence Is Dead!”