The Eisenhower School
for National Security and Resource Strategy

Academic Year 2022
Networking and Communications Technology Industry Study

Final Report:

Networked Power
Addressing the role of networking & communication technologies in 21st-century influence operations

20 May 2022
National Defense University
Fort McNair, Washington, D.C. 20319-5062

Table of Contents

Foreword: *Six Degrees of Connection*

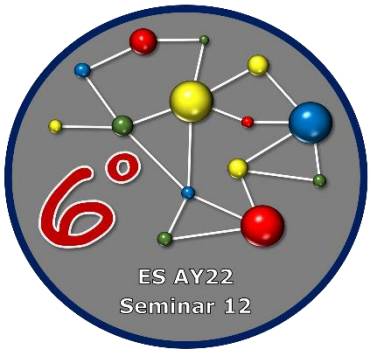
This report concludes a semester-long study by Seminar 12, Networking and Communications Technology (NCT) Industry Study, during academic year 2021-2022 at the Eisenhower School for National Security and Resource Strategy.

Otherwise known as "Six Degrees," shorthand for six degrees of separation, our cohort includes a diverse mix of 17 mid-career professionals from across the Department of Defense (DoD), international military, and U.S. interagency partners. We are active-duty officers from three branches of the U.S. military, including the Reserve Component, foreign military officers representing four allied and partner nations, and career civilians at DoD, the Department of State, the Department of Homeland Security and the General Services Administration. While some in our group had specific backgrounds in communications and influence, given the proliferation of NCT, all had a working knowledge as users, with a basic understanding of the industry's societal and national security impacts.

After courses in the broader Eisenhower School curriculum in Strategic Leadership, Economics, Strategy, Industry Analysis, and Strategic Acquisition, we spent a semester interacting with a broad set of experts in government and industry (see "Outreach and Field Studies").

Our year at the Eisenhower School was a mix of in-person and virtual classes as a result of the ongoing pandemic. This experience shaped our interaction with the curriculum by providing real-world insight into the importance of NCT to enable continued communication and dialogue, particularly when international travel was curtailed. We also saw firsthand the role of NCT in the U.S. departure from Afghanistan in the fall of 2021 and Russia's invasion of Ukraine in 2022.

While the United States and other democracies around the world seek to heal divisions in their populations as they pursue pandemic and economic recovery programs, great power competitors exploit NCT for malign influence purposes. After a semester-long study of challenges and opportunities from the U.S. Government and industry perspective, "Six Degrees" concluded that the continued battle for information supremacy is the defining competition of the 21st century—one that the United States cannot afford to lose. Amid this sense of urgency, we humbly offer the analysis and recommendations in this report.



***Six Degrees* - Seminar 12**

Josue Barrera, Department of State
Lieutenant Colonel Franklin Dennis, U.S. Army
Jared Ford, U.S. Border Patrol
Kelly Hardy, Department of the Navy
Jerome Hohman, Department of State
Tila Kety, General Services Administration
Daniel Kimmage, Department of State
Colonel Irakli Kolbaia, Georgia Army
Lori Leffler, Department of Defense
Colonel Harvey Molope, Botswana Army
Lieutenant Colonel Jake Olson, U.S. Marine Corps
Calvin Peterson, Department of State
Rahman Rahmani, Afghan National Army Aviation
Colonel Megan Schafer, U.S. Air Force
Lieutenant Colonel Nebojsa Stajic, Bosnia and Herzegovina Army
Glenn Tosten, Department of State
Colonel Ifeoma Izuchukwu, U.S. Air Force Reserve

Faculty

Colonel Nancy Blacker, U.S. Army
Colonel Elvert Gardner, U.S. Space Force
Robert Garverick, U.S. State Department
William Soderberg, Federal Bureau of Investigation

Industry Study Outreach & Field Studies

Human networking
– Dr. Jen Golbeck, University of Maryland College of Information Studies

Social Media Platforms
- Susan Benesch, Harvard University, Dangerous Speech Project

Information, Misinformation, Disinformation, and Influence
- Dr. Pablo Breuer, Morgan Stanley
- Gerrit De Vynck, Washington Post
- Andrew Hammond, Spy Museum
- Evanna Hu, Atlantic Council and
- National Counterterrorism Center

Critical Infrastructure
- Tom Miller, Col (Ret) Steve Luczynski, Cybersecurity and Infrastructure Security Agency

Legal Issues
- Gary Brown, NDU CISA
- Scott Chambers, Exercise "Baltic Gavel"

International Partners/NATO
- JJ Green, WTOP Investigative Reporter
- Mr. Michael Ryan, former DASD Europe/NATO Policy, Office of the Secretary of Defense
- John Sunderland, NATO Strategic Communications Center of Excellence
- Lt. Gen. (Ret) Dan Bolger, former Commander of NATO mission in Afghanistan

Field Study 1, Atlanta Georgia
- Dr. Larry Kim, Georgia Tech Research Institute
- High Museum, Disrupting Design: Modern Posters

Field Study 2, New York City, New York
- Ken Klose, Joint Terrorism Task Force, Federal Bureau of Investigations
- Mo Telab, CISA Region 2
- Fernando Puerto-Mendoza, Balquis Al Radawan, United Nations
- Dr. Alexis Wichowski, Dr. Munish Walther-Puri, Pat Meheny, Columbia University
- Rebecca Fisk, Paley Center
- David Shafer, NASDAQ

Field Studies 3, Tampa, Florida
- COL Andrew Whiskeyman, U.S. Central Command J39
- Joint Miso Web-Ops Center
- U.S. Special Operations Command
- Joint Special Operations University

Introduction

Adversaries have long used propaganda, disinformation, and deception to gain an advantage over opponents, shape how they think, control the flow of information, and attempt to win wars without fighting. The evolution of networking and communication technology (NCT) over time has expanded the reach and potential effectiveness of these efforts. Social media has emerged as such a powerful tool that some describe it as a weapon of modern warfare. It doesn't stop there—online messaging, gaming, financial technology, artificial intelligence (AI), and a slew of other NCT have revolutionized the adversary's tool kits for propaganda and deception.

Efforts to influence large populations that previously took decades of activity with significant financial resources and manpower can now happen in days, if not minutes, and at little cost.[1] Governments worldwide are now threatened by the power of NCT and the individuals who can tap into that power. The balance of power is shifting from government to the people, and nefarious attempts to wield that power have become a national security concern. Informational approaches, enhanced by NCT, are often applied in support of other instruments of national power, commonly dominated by diplomatic, military, or economic tools. However, future strategy may warrant an approach that considers information as the supported instrument of national power because it offers the best opportunity to advance U.S. interests without a greater risk of military conflict with Russia or China.[2]

NCT offers a powerful tool to defend against malign influence while safeguarding the democratic values of free nations around the world. It can give a voice to the voiceless in authoritarian regimes and level the playing field against powerful adversaries with considerable influence capabilities and values contradictory to our own. Social media companies, the U.S. government, and many of its allies and partners are unprepared to address these challenges,

despite the known use of NCT by bad actors and perceived societal ills. The United States runs the risk of resorting to ineffective knee-jerk reactions in the name of security. Additionally, ill-informed responses could threaten civil liberties, particularly speech and privacy, and have the potential to create more damaging long-term effects than an adversary's intended harms.

This paper will summarize the semester-long research activities of the NCT industry study through the following structure: an overview of the strategic environment, a definition of the industry, an analysis of NCT and the instruments of power, and finally, recommendations to secure and increase the benefits of a more connected world through regulatory reform, partnership, education, and national strategy.

Strategic Environment

Advances in networking and communications technology have shaped today's world more than almost any other factor. The progression from the earliest prehistoric cave drawings to hand-carried written letters to the telephone and internet has led to an incredibly interconnected world. Major advances in communications technology came thick and fast in the late twentieth and early twenty-first century. Mobile communications raced from 0 generation (0G) to 4G in a relatively short time. The United States, along with many other countries, is now working toward the full implementation of the 5G mobile communication, which will bring unprecedented digital speeds and stronger connectivity for a broader range of devices.[3] The internet of things (IoT) is quickly evolving into the Internet of Everything (IoE), a state of ubiquitous hyper-connectivity.

The scope and speed of communication has changed, but the fundamentals remain the same. Author, message, and audience are still foundational to the exchange of information and ideas, whether online or in person. The advent of the internet and the ability to communicate quickly and easily with people with similar and divergent beliefs, feelings, and opinions globally

has brought undoubted benefits. It has also created an increasingly contentious information domain that poses potential threats to U.S. national security in the form of divisive malicious activity such as disinformation campaigns and dangerous hate speech.

The evolution of communications technology and an increasingly interconnected world have underscored the importance of the gray zone or the "contested arena somewhere between routine statecraft and open warfare."[4] While the United States has been primarily focused on conventional power, Russia, China, and non-state adversaries such as ISIS have exploited the gray zone to pressure, coerce, destabilize, and attack the United States and its allies. Operating in the gray zone through disinformation campaigns and other means is relatively simple and inexpensive. It levels the playing field significantly, reducing the United States' advantage in conventional military capability.

Over the past two decades, Russia's security services and military have developed a considerable networking and communications technology toolset that, along with effective control over criminal hacker groups, places Russia at the top of global "gray-zone" threats. President Vladimir Putin's regime has put that capacity to work to steal sensitive data, compromise computer networks, carry out divisive influence campaigns, and weaken the governments of rivals and neighbors as part of an ongoing "war" against the West and the forces of democracy.

Democracies believe that freedom of expression and access to information empowers citizens and facilitates progress. They are willing to take risks with security and control. Authoritarian governments—including China, Russia, and some oil-rich monarchies—prioritize control and censorship, often in the name of security.

The utility of social media and other communications platforms as a military and political tool is increasingly apparent. The resulting national security threats to the United States cannot be dismissed. The weaponization of networking and communications platforms has caused myriad negative impacts on society, such as mental health deterioration, civil unrest, loss of trust and confidence in government institutions, and even war. At the same time, the opportunities afforded by new technologies can be a boon to U.S. national security. A greater understanding of NCT as an industry is critical to charting a way forward to address these challenges.

The Industry Defined

NCT is a young, rapidly growing industry that resists easy categorization. Networks can be defined as complex systems consisting of nodes and edges.[5] For example, nodes represent individuals, and edges represent the interactions between individuals.[6] Humans have formed networks like this throughout history. Humans have a basic psychological need for love and belonging, which suggests that they will continue forming networks long into the future.[7]

To form networks, humans need to be able to communicate. This can be as simple as two people speaking with one another over dinner. They can also use communications technology or the tools used to send, receive, and process information.[8] Today, communications technology broadly refers to the huge number of electronic devices across the world, networked together via access to the internet.[9]

For the purposes of this study, NCT refers neither to the internet and the internet of things nor to human social interaction but the tangled intersection of both. Researchers continue to establish the characteristics of the industry, its components, and their interrelationships. As of this writing, a common worldwide understanding and widespread agreement on these characteristics have proved elusive. This study considers NCT as the sum of technologies and

interactions that make up the global information environment. The authors acknowledge and appreciate other, potentially dissenting, perspectives that may exist.

The structure of the NCT industry is complex and diverse. In an increasingly globalized and ever-changing strategic environment, people, devices, and information are networked across multiple industries and domains. NCT industry participants include individual users, private sector companies, government agencies, and non-state actors. The industry includes social media and cyber security, and it links all 16 officially recognized components of U.S. critical infrastructure.

The large conglomerates currently dominating private sector business in the NCT industry have found lucrative opportunities in a world where so many interactions and transactions occur on an unprecedented scale. For example, Google and Meta (formerly Facebook) make their platforms available at no monetary cost to users. They collect and analyze the data (and metadata) willingly provided by individuals to enable targeted advertising to their paying customers.

The collection and analysis of so much data is clearly useful for private companies, but it presents privacy and information security challenges. The same information that allows for targeted consumer advertising is also attractive to criminals, foreign adversaries, malicious hackers, and other nefarious actors.

Domestic and international regulatory bodies have taken a keen interest in the NCT industry. The United States has reevaluated regulations multiple times in recent decades.[10] Most recently, U.S. officials engaged in consequential discussions and sometimes contentious dialogue about antitrust, competition, and Section 230 of the Communications Decency Act of 1996.[11] Section 230 is particularly relevant to the industry because it frees online platforms from liability

for third-party content. While the United States struggles to address emerging NCT issues domestically, there is also a need to establish global norms and agreements in light of the industry's global presence.

The following analysis reviews the role of NCT in the instruments of national power with an eye to the critical challenges and opportunities present in today's hyperconnected world.

Diplomacy

Networking, communications, and the information domain have emerged as an increasingly important area of diplomacy in recent decades. The Department of State devotes considerable attention to them, but they command fewer resources overall than their prominent role as drivers of societal change and international relations might warrant.

The Department of State is far from the only U.S. government entity to use communications, but it is almost certainly the component that uses information-related tools most actively to carry out its mission. Many U.S. government actions resonate in the information space—for example, Department of Defense freedom of navigation operations, aid and assistance, and law enforcement actions outside of the United States—but the Department of State is ultimately responsible for any consequences these operations and activities might have for bilateral relationships. For this reason, U.S. government messaging needs to be coordinated through the Department, particularly through embassies, which are best placed to gauge local politics and sensitivities.

Embassies are where most U.S. government communications happen. The National Security Council and other Washington-based offices make policy and guidance, but the U.S. government's frontline communicators are in the field. Their knowledge of local dynamics is key to delivering messages to target audiences in ways that ensure positive resonance.

The core of the State Department's communications capabilities is located in the offices overseen by the Under Secretary for Public Diplomacy and Public Affairs. They focus on public affairs, educational and cultural exchanges, data analytics, and counter-disinformation. Their activities go beyond messaging to include a wide array of person-to-person contacts and networks of individuals and organizations. The regional bureaus, overseen by the Under Secretary for Policy, also have a crucial role to play. They help set policy; more importantly, they run the Department's global network of embassies.

Most of the institutional architecture for public diplomacy migrated to the Department of State in 1999 when Congress dissolved the U.S. Information Agency. The Department's embrace of this function has led some critics to doubt its commitment. The office of the senior official overseeing public diplomacy has been vacant almost as often as it has been filled over the last two decades.[12] The current annual budget for public diplomacy is around $1.4 billion, with approximately half of that going to fund exchanges.[13]

On any given day, the U.S. government component most likely to send a message that reaches an ordinary citizen outside of the United States is international broadcasting, which has a daily audience of millions of viewers and listeners. It includes the Voice of America and Radio Free Europe/Radio Liberty, which made a name for themselves during the Cold War, as well as more recent creations such as Middle East Broadcasting and Radio Free Asia. The U.S. Agency for Global Media oversees the broadcasters. It is an independent agency with a budget of around $800 million, but its leadership coordinates with the Department of State on strategic issues.[14] A legislative "firewall" protects the journalistic integrity of the broadcasters.

Despite its recognized importance, the U.S. government does not emphasize information in strategy, nor has it considered a separate strategy for information. The Interim National

Security Strategic Guidance issued by the Biden administration in 2021 only mentions the subject in passing, generally in the context of threats from adversaries or the commercial opportunities of new technologies. Some countries are moving toward the use of separate strategies in this area.[15] For example, Russia issued an Information Security Strategy in 2016 that sets national priorities and lays out a framework for whole-of-government coordination.[16]

The U.S. government's response to Russia's full-scale invasion of Ukraine in February 2022 made full use of the instruments surveyed above. The Department of State provided daily briefings for the media, sometimes showcasing declassified intelligence that exposed Russian plans and inoculated audiences against Russian disinformation. The Global Engagement Center released reports identifying and debunking specific instances of disinformation.[17] International broadcasting stepped up its activities in Russia and actively employed technologies such as virtual private networks to help listeners overcome Russian government attempts to block access to alternative sources of information online.[18]

These recent successes in countering malign influence from Russia may serve as a tremendous opportunity to advocate for additional resources, both in the form of manpower and funding, or prioritization, in the form of emphasis in national strategy.

Information

As previously noted, the United States does not have a strategy specifically for the information instrument of power. Many analysts agree that the United States has not excelled in the information space and that it also shares the inherent vulnerabilities of free and open societies.[19]

Like other free nations, the United States values the civil liberties of its citizens. This is a foundational philosophy embedded in the Constitution and the institutions of the U.S.

government. While it is not uncommon for democracies to accept some infringement on civil liberties for short-term security considerations, long-term infringements in the form of norms, laws, or policies are not acceptable. Meanwhile, the global access and connections provided by NCT have enabled authoritarian regimes to weaponize misinformation and disinformation against the United States while also controlling the flow of information to their populations.[20]

The use of information as a power projection tool and the ability to exploit NCT are crucial to success in today's global power competition. Technological advances have expanded the scope of great power competition well beyond the military instrument of power. While the United States was focused on counterinsurgency and counterterrorism operations, adversaries like Russia and China developed and began implementing sophisticated hybrid warfare strategies.[21]

Russia, China, and other adversaries have capitalized on emerging communication technologies as a way to attack democratic vulnerabilities and win without direct military confrontation. They undermined U.S. influence via information operations, cyber warfare, social media exploitation, and other NCT-enabled hybrid tactics. At the same time, the United States was immersed in counterinsurgency operations and attempts to mitigate the global terrorist threat. Making U.S. society more resistant to hybrid threats is essential for enhanced security.

While President Biden's *Interim National Security Strategic Guidance* mentions resilience as relevant to national security concerns, the Department of Homeland Security's most recent Strategic Plan strongly emphasizes the concept.[22] Indeed, resilience is an increasingly popular topic of discussion in U.S. national security circles.

A 2021 study of Western democracy vulnerabilities to hybrid warfare posits that resilience is the key strategic concept in defending against cyber and information warfare while

upholding democratic values.[23] The study notes that "[i]nvestment in education is the most efficient way to increase [a] state's resilience" while also calling attention to other concepts like critical thinking, public-private partnerships, and government transparency.[24] Another study reinforces existing research findings that public trust and individual resilience levels are effective predictors of national resilience.[25]

A nation can defend itself against malign influence by developing the individual resilience of its citizens and building their trust. In today's digitized information domain, this can be accomplished by: 1) investing in education; 2) promoting critical thinking; 3) fostering situational awareness; 3) developing cooperative intra- and interrelationships across public and private sectors; 4) advancing cybersecurity capabilities; and, 5) maintaining transparency to the extent possible.

Military

NCT has leveled the playfield. In Ukraine, Russia's large-scale conventional force is sustaining a serious challenge from a high-tech, individual networked adversary. While this has become widely understood in combat scenarios, thanks to the successful application of NCT in counterterrorism operations, its applicability to competition in the gray zone warrants greater attention.

The gray zone's basic definition is the operational space between peace and war.[26] Common characteristics and strategies of gray zone operations include:

- Using a variety of means to undermine adversary power and influence while building one's own;
- Employing strategic ambiguity to favorably shift the power balance;
- Operating across multiple domains and instruments of power;

- Ensuring activities remain below the threshold of conventional war;
- Obscuring the lines between military and non-military action, as well as peacetime operations and warfare; and,
- Taking measures to avoid attribution.[27]

Several NCT constructs—e.g., fake social media accounts, gaps in cybersecurity, general interconnected but malleable structure, etc.—promote or at least support ambiguity and actor anonymity. The interconnected nature of NCT also presents myriad opportunities to exploit vulnerabilities, even against adversaries who hold a clear advantage.

Nowhere is this more apparent than in recent events in the ongoing Russia-Ukraine conflict. Russia has a significant military advantage over Ukraine, yet it has not achieved the success Vladimir Putin anticipated, and certainly not in the time frame he preferred. NCT played a vital role in Ukraine's ability to persevere against a more powerful adversary. Starlink has played a pivotal role in keeping Ukrainians connected to the larger global network.[28] This capability enables other essential communication functions as well. Ukrainian citizens can receive information to stay informed and send communications, including photographs and videos documenting their experiences. The Russia-Ukraine conflict is a current event that perfectly exemplifies the magnitude of impact NCT can have even in a conventional war.

Economic

The economic instrument of power exhibits several impacts of networking and communications technology on U.S. national security. First, the United States, Russia, and China gather and utilize data to gain economic power. Second, economically relevant critical infrastructure sectors such as the financial sector are impacted by continual cyber threats and the resulting investments needed to secure information technology. Third, the rise of China's

economic power and its influence on the U.S. entertainment industry has concerning implications for U.S. national security.

Data gleaned through information technology is the new currency in an interconnected world, where it is driving economic growth, power, and influence. Data can be collected, analyzed, monetized, and used to identify weaknesses and undermine adversaries. The intertwining of economies worldwide means almost all nations are now more dependent on one another. This entanglement presents opportunities for rapid wealth accumulation, the sharing of new technologies, and soft power deployment.

Understanding how data is collected and handled through information technology is vital to ensuring national security, especially in the digital advertising market. Collecting, sharing, and utilizing consumer data without regard to privacy will reduce public trust and increase national security vulnerabilities. Data is vital to big tech and social media companies that primarily make money through digital advertising. The data these companies collect from their billions of users allows them to target ads more effectively. Big tech's business model encourages the employment of psychological and propaganda methods to increase their share of the "attention market"—the time users spend on their platforms.[29] Firms are, however, understandably resistant to changes to their business model, including increased government regulation or the imposition of liability for third-party content that might impact profitability.

Democracies are now struggling to balance broad access to the internet and free speech with privacy concerns and efforts to counter malign influence campaigns. Russia and China use social media companies' algorithms to target specific groups of people for influence campaigns. This has led many to suggest requiring more transparency and accountability from the social media companies. Others have questioned whether Section 230 of the Communications Decency

Act, which absolves social media companies of responsibility for the material users post online, should be revised or thrown out.

Another area where information technology has increased importance is the defense of U.S. critical infrastructure. Over 300,000 new pieces of malware are created, and more than 2,200 cyber-attacks occur daily in the U.S.[30] Cyber-attacks are estimated to cause breaches that cost companies around the world $6 trillion to fix in 2021.[31] Cyber-attacks on critical infrastructure can lead to the loss of intellectual property and personal information. They can also impact the supply of oil, gas, water, or food. The United States has identified 16 critical infrastructure sectors for protection. Information Technology has been identified as essential to the protection of all the other sectors. as it could be used as a tool to disrupt or disable targets. It is the hub connecting all the others.[32] The financial services sector is particularly vulnerable. Stock trading services face dozens of attempted hacks every day, and large and vital financial corporations such as NASDAQ must invest heavily in information security.

Lastly, the power of cinema in the ideological competition between states creates opportunities to reach the hearts and minds of people. China has invested heavily in the U.S. entertainment industry, and the size of its domestic market has begun to exert a gravitational pull on movie producers. U.S. producers are altering films to positively portray China, either at the demand of investors or to appease the Chinese Communist Party and to secure access to the booming Chinese market.[33]

Law Enforcement

It is no surprise that NCT creates tremendous opportunities and significant challenges for law enforcement, particularly in balancing civil liberties and Constitutional rights in open democracies like the United States. Bureaucratic processes—including regulation and other

activities inherent to legal proceedings—are simply unable to keep up with the accelerating change of technology.

The killing of George Floyd was captured on a smartphone camera by a young teenage girl. The smartphone connected the girl to the internet, including social media and other communication platforms, where she could share the video, making it instantly accessible to millions of others. The cascading events that followed—from the video "going viral," to protests, civil unrest, unprecedented political polarization, and the unraveling of deep-seated contempt for government authority—all happened because of a few finger-taps on a mobile phone.[34] Public opinion shifted because of the video's wide reach and the resulting prosecution of the case involving Floyd's death, bringing attention to allegations of systemic racism across the nation. This is an extreme but real example of NCT's impact on law enforcement and government.

Another contentious issue American legislators and law enforcement professionals face revolves around the First Amendment. Among other liberties, this Amendment affords U.S. citizens the freedom to express themselves by any means, regardless of the content or popularity of said expression, so long as it neither involves criminal activity nor provokes others to engage in criminal activity—especially that which culminates in violence. Thus, a degree of hate speech is entirely legal in the United States.[35] Challenges appear in distinguishing between the legality of hate speech and the illegality of dangerous speech. Susan Benesch, the founder of the Dangerous Speech Project, defines dangerous speech as "any form of expression (speech, text, or images) that can increase the risk that its audience will condone or participate in violence against members of another group."[36] This can include some forms of hate speech as well.

While legal institutions struggle to achieve a common understanding of basic term definitions, law enforcement professionals are forced to make snap decisions without established

legal foundations or judicial system support. The consequence of just one mistake or incorrect decision carries the risk of bystanders distributing the news and photographic proof across their communities and to any number of people around the world.

Cybercrime presents its own set of challenges for law enforcement, with a magnitude equivalent to that of free speech. The emergence of new or improved communication technologies and the expansion of digital social networking has outpaced the ability of government institutions, including law enforcement, to develop systems of governance for the new patterns and paradigms.[37] Until such governance systems are developed, law enforcers find themselves in a precarious situation. They must learn how to effectively police and prevent crimes that exploit the new, malleable cyber domain. This includes entirely new types of crimes like ransomware attacks.

From a legislative perspective, there is no shortage of problems requiring attention, although some of these problems present a similar legislative challenge. Decision-makers must overcome relative ignorance of the technology and its more significant implications to the social, political, economic, or other defined environment. The World Economic Forum recognizes this issue and posits that the best way to approach regulation in a complex environment is with a solid foundation of values instead of pursuing the impossible goal of matching the speed of regulation to the speed of technological advance.[38]

Intelligence

The revolution in communications technology has created unprecedented opportunities for open-source intelligence collection. Some of these have translated into threats to U.S. national security. When information about workouts was shared by users of the fitness app Strava gave away the locations of previously unknown U.S. military facilities overseas.[39] Others

have translated into gains for U.S. allies, as when the United Kingdom was reportedly able to track Russian troop movements through data soldiers inadvertently shared on dating apps.[40]

As practiced by highly skilled non-governmental organizations like Bellingcat, open-source intelligence plays a crucial role in bringing war crimes and atrocities to light. Bellingcat successfully identified the Buk missile launcher that downed Malaysia Airlines Flight 17 in 2014, thwarting Russian attempts to obfuscate the actual perpetrators of the crime.[41]

New communications technology is revolutionizing the collection and subsequent analysis of imagery. Cheap drones and high-resolution cameras can gather enormous amounts of previously inaccessible data, while artificial intelligence can discover patterns invisible to human analysts. The dangers of these advances are evident in their misuse in authoritarian regimes like China, enabling invasive surveillance of the Uighur minority.[42] Related technologies can produce doctored images, audio, and even computer-generated texts to misinform and mislead.[43]

The U.S. intelligence community has struggled to integrate these new capabilities harmoniously. The sheer profusion of open sources, the confusing array of proprietary interfaces associated with social media platforms, and the closed nature of the community's internal systems have all emerged as obstacles. Stovepipes within a sprawling and highly specialized community are another impediment.

Recommendations

The enormous complexity of the information domain makes it challenging to offer recommendations for the U.S. government. NCT is not an industry with easily measured outputs, nor is its relationship with the U.S. government like industries that supply weapons or vital materials. NCT resembles a combination of geography, topography, and weather in that it shapes

the very environment we inhabit in its prevalence, permanence, and ability to change. Government cannot control it but has tools to affect it.

The following recommendations are grouped under the general rubrics of regulatory reform, partnership, education, and national strategy. In most cases, they identify areas that deserve heightened focus rather than specific actions that need to be taken.

Regulatory Reform

Social media companies must take greater responsibility for the content on their platforms. The content draws users, who provide data, which makes the companies rich, but the cost to society has increasingly taken the form of division and disinformation. By all indications, the cost is rising.

Section §230 of the Communications Decency Act of 1996 can lay claim to being considered the economic engine of the internet. It frees platform providers from liability for content posted on their platforms. Without it, social media companies would face ruinous lawsuits or the prospect of hiring vast compliance staff. In its current form, it allows some of the wealthiest and most powerful entities on earth to evade responsibility for activities that are highly beneficial to them yet highly damaging to society.

The trick will be to amend Section 230 in a way that pushes companies toward greater social responsibility without wrecking their bottom line. NCT has improved the quality of human existence, sparked unprecedented innovation, and powered economic growth. These are not trivial gains. Changes will need to be carefully calibrated to keep the regulatory burden as light as possible while incentivizing companies to end the free-for-all that has allowed Russian operatives, foreign and domestic extremists, and common criminals to run amok on platforms.

This paper does not purport to solve the dilemmas that surround the reform of Section 230. What it recommends is higher-level attention to the issue in the executive branch, which should deliver to citizens and legislators a clearer analysis of the negative consequences of the status quo for our national security and the legislative branch, which must eventually take action to solve the problem.

Partnerships

By their very nature, networks create partners. The United States should make more active use of partnerships to deepen our understanding of NCT and organize common action on threats and opportunities. For example, the NATO Science and Technology Organization includes a community of more than six thousand scientists. It draws on the expertise of more than 200,000 people in NATO to collaborate on research. The U.S. government should take the lead in establishing a formal, NCT-focused partnership with the NATO Science and Technology Organization, setting a research agenda, and providing funds for new initiatives while asking other NATO countries to do the same.

The National Science and Technology Council should augment its six committees with a seventh committee on partnerships.[44] The new committee should gather recommendations from the six standing committees—which focus on the science and technology enterprise, environment, homeland, and national security, science, STEM education, and technology—on current partnerships, new opportunities, and steps that need to be taken to broaden collaborative work on NCT with other governments and non-government organizations, both at home and abroad.

The Council should also draw up a list of all components within U.S. government departments and agencies with a significant stake in NCT and task them with producing a list of

their current partnerships, opportunities for new partnerships, and any obstacles to their creation. The Council should work with the National Security Council and Congress to set targets to increase the number of partnerships and overcome hurdles that might prevent this.

Education

The 2021 Interim National Security Strategic Guidance rightly prioritizes STEM education. It states, "We will expand our science and technology workforce by investing in STEM education, where America is currently losing ground."[45] The U.S. government should augment this effort, particularly in the K-12 curriculum, with an educational component focused on NCT and the information environment.

Topics to be covered should include the core technologies in NCT, media literacy, cyber hygiene, and practical skills to recognize disinformation campaigns. Countries like Finland have already expanded school curricula to integrate this material.[46] The Department of Education should work with the Department of State to compile a list of international programs that could serve as examples and a team of educators to develop additions to the U.S. curriculum.

National Strategy

The information domain and NCT are treated as an afterthought in current U.S. strategies like the National Security Strategy. This approach has not borne fruit. The National Security Council should produce a short unclassified document on NCT and the information domain that lays out the global context, sets U.S. national priorities, and identifies tangible goals and steps to be taken. A classified version could focus in more detail on adversarial threats, U.S. vulnerabilities, and mitigation measures.

Conclusion

The ongoing battle for information supremacy is the defining competition of the 21st century—one the United States, and its allies and partners, cannot afford to lose. One need not look further than the war in Ukraine to see a paradigm shift in the information space. Ordinary citizens can now balance the power and influence of hostile states.

At a time of economic turmoil and divided foreign policy commitments, the United States must consider how information can serve as the supported instrument of national power. It may be one of the best tools to counter adversary malign influence, advance U.S. interests, and defend democratic values.[47]

As Benjamin Franklin famously declared, we have "a republic, if you can keep it." If applied, the lessons learned from NCT's impact on influence operations from competition to conflict can serve to benefit and protect the security and rights of our citizens. The dynamic, confusing world of networking and communications technology is often presented as a problem, but it can be a solution—if we let it.

Appendix – Lessons Learned in Ukraine

For all its focus on information tools as an instrument of power, Russia's vaunted cyber capabilities have not had the devastating impact expected by many cybersecurity experts and media pundits in advance of the 2022 Russian invasion. It is true that Moscow has deployed significant elements of its cyber and hybrid resources to attack Ukraine. However, it is uncertain thus far just what the impact of Russia's cyber and influence campaign – as part of a multidomain assault on Ukrainian government, military, and civilian targets – has been, leaving many observers questioning the conventional wisdom that Moscow could and would unleash an overpowering cyber assault with visible impact on Ukraine.

Moscow ramped up its cyber and information warfare operations against Kyiv in the weeks leading up to the 2022 Russian attack on Ukraine.[48] Likely Russian or Russian-allied actors hacked Ukrainian government websites on several occasions in mid-January 2022; in one instance posting an ominous warning on a government webpage: "Be afraid and expect the worst." In the same period, Microsoft announced it had discovered the presence of malware intended to wipe the records of dozens of Ukrainian government offices, which would have left those systems inoperable. The Ukrainian government acknowledged in mid-February that its Defense Ministry systems had been hit with a distributed denial of service (DDOS) attack, which was later attributed to the GRU. Additionally, declassified U.S. intelligence in the same timeframe revealed that dozens of other Ukrainian government systems had been penetrated with malware waiting to be activated at the start of the Russian attack. Further malware incursions and hacks against Ukrainian systems were reported throughout February, March, and April 2022. This includes an attack against global satellite communications company Viasat, which was

targeted with a complex DDOS hack intended to disrupt Ukrainian government and military communications during the February 24 launch of the Russian assault on Ukraine.[49]

In response, the Ukrainians deployed markedly different tactics than Moscow in seeking to counter Russian cyber and influence operations. In addition to employing standard technical measures meant to resist and prevent Russian cyber incursions, the Ukrainians have called on the international community of information technology experts and hackers to aid them by infiltrating and disrupting Russian military and infrastructure targets.[50] So-called "hacktivist" groups like "Anonymous" have carried out attacks on dozens of Russian government websites to post details about the progress of the war, steal and publicize Russian Ministry of Defense data, and broadcast battlefield images over Russian television to a poorly informed Russian public.[51]

Kyiv's approach to cyber operations in response to the Russian attack fits within its broader information warfare and messaging strategy, which has been in operation over many months, including throughout the 2021 Russian buildup of military forces along Ukraine's borders. In implementing this strategy, Ukrainian President Volodymyr Zelinskiy and his government have waged an effective influence campaign intended to elicit global sympathy for their cause and assistance for their military, as outlined by Yale researcher and U.S. information warfare officer Torey McMurdo in a March 2022 assessment for the Washington Post.[52]

The early results of information warfare have largely favored Kyiv. The lessons of the first six weeks might be summarized as follows:

- Leadership matters. President Zelenskyy's courage and openness have been far more effective than President Putin's cautious formality, particularly with European and American audiences. The close correlation between the Ukrainian president's deeds and words enhanced his credibility, which brought tangible benefits to Ukraine in the form of aid and

sanctions. Putin's obsession with historical minutiae fell flat outside of Russia.

- Civil society is a major asset. Ukrainian government communicators made effective use of social media, but the biggest viral successes—memes of Ukrainian farmers towing away captured Russian military equipment, for example—came from individuals unaffiliated with the government.
- Many experts made dubious assumptions. Russian information operations stumbled. Cyber war didn't happen. Ukrainian society consolidated in wartime. Much of this ran counter to received wisdom before the war.
- Acumen outweighs technology. Pro-Ukrainian voices made masterful use of social media by leveraging linguistic and visual creativity, not sophisticated technical tools. Artificial intelligence, machine learning, natural language processing and deep fakes played no discernable role.
- Authoritarian governments are making better digital iron curtains. Russia and China have invested in propaganda, instituted repressive measures, and used technical means to shape the information environment for the majority of their citizens. The balance of power in the information environment within authoritarian states is now tilted in favor of governments, not the forces that seek to ensure greater freedom.
- Reality matters. Russian narratives that denied battlefield failings or atrocities ran into a buzzsaw of documentary evidence that made a mockery of Russian claims. Only in the walled garden of its domestic information environment could Moscow tell a story unencumbered by facts and unchallenged by alternatives.
- Truth is (still) a casualty of war. Ukraine's broad narrative was more broadly truthful than Russia's, but specific elements did not hold up to scrutiny. The "ghost of Kyiv," a fighter

pilot who supposedly downed multiple Russian jets, and the Snake Island soldiers, who chose death over surrender, are both examples of traditional wartime propaganda crafted to boost morale.[53]

---

[1] Galeotti, Mark. *The Weaponisation of Everything; A Field Guide to the New Way of War*. Yale University Press, 2022.
[2] "Harnessing the Power of Information: A Better Approach for Countering Chinese Coercion," National Defense University Press, accessed May 18, 2022, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2497080/harnessing-the-power-of-information-a-better-approach-for-countering-chinese-co/.
[3] "5G, Explained," MIT Sloan, accessed April 24, 2022, https://mitsloan.mit.edu/ideas-made-to-matter/5g-explained.
[4] "Gray Zone Project | Center for Strategic and International Studies." Center for Strategic & International Studies, 2019. https://www.csis.org/programs/gray-zone-project.
[5] Santa Fe Institute, *Raissa D'Souza - "The Science of Networks" (C4 Public Lectures)*, 2019, https://www.youtube.com/watch?v=a6U7ksiu10Y.
[6] "Edge Definition - Math Insight," accessed May 15, 2022, https://mathinsight.org/definition/network_edge.
[7] A. H. Maslow, "A Theory of Human Motivation," *Psychological Review* 50, no. 4 (1943): 370–96, https://doi.org/10.1037/h0054346.
[8] Mary Clare Novak, "Communication Technology: What Is ICT and Its Components," accessed May 15, 2022, https://learn.g2.com/communication-technology.
[9] Gwanhoo Lee, "What Roles Should the Government Play in Fostering the Advancement of the Internet of Things?," *Telecommunications Policy* 43, no. 5 (2019): 434–44, https://doi.org/10.1016/j.telpol.2018.12.002.
[10] For one example, see "Cybercrime and the Law: Computer Fraud and Abuse Act (CFAA) and the 116th Congress," CRS Report (Congressional Research Service, September 21, 2020), https://crsreports.congress.gov.
[11] "Department of Justice's Review of Section 230 of the Communications Decency Act of 1996," June 3, 2020, https://www.justice.gov/archives/ag/department-justice-s-review-section-230-communications-decency-act-1996; "What Happened the Last Time Congress Amended § 230," Lawfare, March 15, 2022, https://www.lawfareblog.com/what-happened-last-time-congress-amended-%C2%A7-230.
[12] Matt Armstrong, "It Is Time to Do Away with the Under Secretary for Public Diplomacy," *MountainRunner* (blog), January 14, 2022, https://mountainrunner.us/2022/01/abolish-public-diplomacy/.
[13] *2021 Comprehensive Annual Report on Public Diplomacy & International Broadcasting* (Washington, DC: U.S. Advisory Commission on Public Diplomacy, 2021), 3.
[14] *2021 Comprehensive Annual Report on Public Diplomacy & International Broadcasting*, 297-298.
[15] *Interim National Security Strategic Guidance*. Washington, D.C.: White House, 2021. https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.
[16] Office of the President of the Russian Federation. *Доктрина информационной безопасности Российской Федерации [Information Security Doctrine of the Russian Federation]*. Russian Foreign Ministry, 2016. https://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163?p_p_id=101_INSTANCE_CptICkB6BZ29&_101_INSTANCE_CptICkB6BZ29_languageId=ru_RU.
[17] United States Department of State. "Vladimir Putin's Historical Disinformation," May 6, 2022. https://www.state.gov/disarming-disinformation/vladimir-putins-historical-disinformation/.
[18] Gramer, Amy Mackinnon, Robbie. "West Seeks to Pierce Russia's Digital Iron Curtain." *Foreign Policy*, April 8, 2022. https://foreignpolicy.com/2022/04/08/west-russia-digital-iron-curtain-media/.
[19] David Ignatius, "Why America Is Losing the Information War to Russia," *Washington Post*, September 3, 2019, https://www.washingtonpost.com/opinions/why-america-is-losing-the-information-war-to-russia/2019/09/03/951f8294-ce8e-11e9-b29b-a528dc82154a_story.html; Jude Blanchette and Seth G. Jones, "The U.S. Is Losing the Information War With China," *Wall Street Journal*, June 16, 2020, sec. Opinion, https://www.wsj.com/articles/the-u-s-is-losing-the-information-war-with-china-11592348246.

[20] "Interim National Security Strategic Guidance," The White House, March 3, 2021, https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.
[21] Matthew Ivey, "It's Time to Stop Pivoting: Great Power Competition Is Everywhere," *Global Security Review* (blog), January 3, 2022, https://globalsecurityreview.com/time-to-stop-pivoting-great-power-competition-global/; Bridget Bachman, "Hybrid: An Adjective Describing the Current War," *Small Wars Journal*, March 25, 2021, https://smallwarsjournal.com/jrnl/art/hybrid-adjective-describing-current-war.
[22] "Interim National Security Strategic Guidance"; Department of Homeland Security, "DHS Strategic Plan: Fiscal Years 2020-2024" (Department of Homeland Security, 2019), https://www.hsdl.org/?abstract&did=826968.
[23] Tuukka Elonheimo, "Comprehensive Security Approach in Response to Russian Hybrid Warfare," *Strategic Studies Quarterly* 15, no. 3 (September 22, 2021): 129. Although achieving widespread agreement on definitions has proven elusive, there is general acceptance that misinformation refers to inadvertent amplification of false information, disinformation refers to the spread of false information with malicious intent, and malinformation is based on fact but maliciously taken out of context. For more, see Cybersecurity and Infrastructure Security Agency, "Mis, Dis, Malinformation," CISA, accessed May 16, 2022, https://www.cisa.gov/mdm.
[24] Elonheimo, "Comprehensive Security Approach in Response to Russian Hybrid Warfare," 129–30.
[25] Daphna Canetti et al., "What Does National Resilience Mean in a Democracy? Evidence from the United States and Israel," *Armed Forces & Society: An Interdisciplinary Journal* 40, no. 3 (July 1, 2014): 504.
[26] Jr. Leimbach Wendell B. and Susan D. Levine, "Winning the Gray Zone: The Importance of Intermediate Force Capabilities in Implementing the National Defense Strategy," *Comparative Strategy* 40, no. 3 (May 4, 2021): 223–34, https://doi.org/10.1080/01495933.2021.1912490; Lyle J. Morris et al., *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War* (Santa Monica, CA: RAND Corporation, 2019), 8, https://doi.org/10.7249/RR2942.
[27] Morris et al., *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War*, 8.
[28] "Elon Musk's Starlink Internet Becomes a Lifeline for Ukrainians," NBC News, accessed May 17, 2022, https://www.nbcnews.com/tech/security/elon-musks-starlink-internet-becomes-lifeline-ukrainians-rcna25360.
[29] Emilia Kirk, "Council Post: The Attention Economy: Standing Out Among The Noise," Forbes, accessed May 19, 2022, https://www.forbes.com/sites/forbesbusinessdevelopmentcouncil/2022/03/23/the-attention-economy-standing-out-among-the-noise/.
[30] "Significant Cyber Incidents | Center for Strategic and International Studies," accessed December 5, 2021, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.
[31] "Deputy Attorney General Rod J. Rosenstein Delivers Remarks at the Cambridge Cyber Summit," October 4, 2017, https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-cambridge-cyber-summit.
[32] Cybersecurity and Infrastructure Security Agency, "Introduction to the Information Technology Sector Risk Management Agency," accessed May 19, 2022, https://www.cisa.gov/publication/information-technology-sector-risk-management-agency.
[33] Stone Fish, Isaac, "How China gets American companies to parrot its propaganda," *The Washington Post*, October 11, 2019, https://www.washingtonpost.com/outlook/how-china-gets-american-companies-to-parrot-its-propaganda/2019/10/11/512f7b8c-eb73-11e9-85c0-85a098e47b37_story.html.
[34] "KARE 11 Investigates: What If There Wasn't Cellphone Video of Floyd's Death?," kare11.com, June 8, 2020, https://www.kare11.com/article/news/local/george-floyd/kare-11-investigates-what-if-a-there-wasnt-cellphone-video-of-floyds-death/89-785d4021-151f-4cb5-8628-f945af01068c.
[35] Although hate speech is not formally defined, it commonly refers to contemptuous or vitriolic expression grounded in an individual's membership in one or more identified protected classes. See: Caitlin Ring Carlson, "Exploring Legal Responses to Hate Speech in the United States," *University of Baltimore Journal of Media Law & Ethics* 8, no. 1 (2020): 32.
[36] "What Is Dangerous Speech?," Dangerous Speech Project, October 27, 2016, https://dangerousspeech.org/about-dangerous-speech/.
[37] Camino Kavanagh, "New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?," Carnegie Endowment for International Peace, accessed May 17, 2022, https://carnegieendowment.org/2019/08/28/new-tech-new-threats-and-new-governance-challenges-opportunity-to-craft-smarter-responses-pub-79736.

[38] Daniel Malan, "The Law Can't Keep up with New Tech. Here;s How to Close the Gap," World Economic Forum, accessed May 17, 2022, https://www.weforum.org/agenda/2018/06/law-too-slow-for-new-tech-how-keep-up/.
[39] Hsu, Jeremy. "Strava Data Heat Maps Expose Military Base Locations Around the World." *Wired*, January 29, 2018. https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/.
[40] Republic World. "UK Spies Track Russian Troops through Dating App Grindr & Social Networking Sites: Report," March 6, 2022. https://www.republicworld.com/world-news/russia-ukraine-crisis/uk-spies-track-russian-troops-through-dating-app-grindr-and-social-networking-sites-report-articleshow.html.
[41] Croxton, Will. "How Bellingcat Tracked a Russian Missile System in Ukraine." *CBS News*, February 23, 2020. https://www.cbsnews.com/news/how-bellingcat-tracked-a-russian-missile-system-in-ukraine-60-minutes-2020-02-23/.
[42] Mozur, Paul. "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority - The New York Times." *New York Times,* April 14, 2019. https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html.
[43] Knight, Will. "AI Can Write Disinformation Now—and Dupe Human Readers." *Wired*, May 24, 2021. https://www.wired.com/story/ai-write-disinformation-dupe-human-readers/.
[44] For more on the council, see: https://www.whitehouse.gov/ostp/nstc/.
[45] *Interim National Security Strategic Guidance*. Washington, D.C.: White House, 2021, 17. https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.
[46] The Nordic Policy Centre. "Media Literacy Education in Finland," November 12, 2020. https://www.nordicpolicycentre.org.au/media_literacy_education_in_finland.
[47] "Harnessing the Power of Information: A Better Approach for Countering Chinese Coercion," National Defense University Press, accessed May 18, 2022, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2497080/harnessing-the-power-of-information-a-better-approach-for-countering-chinese-co/.
[48] Cynthia Brumfield. "Russia-Linked Cyberattacks on Ukraine: A Timeline." CSO Online, April 1, 2022.
[49] Mark Kleinman. "Satellite Giant Viasat Probes Suspected Broadband Cyberattack Amid Russia Fears." Sky News, February 28, 2022. https://news.sky.com/story/satellite-giant-viasat-probes-suspected-broadband-cyberattack-amid- russia-fears-12554004.
[50] Kyle Fendorf and Jessica Miller. "Tracking Cyber Operations and Actors in the Russia-Ukraine War." Council on Foreign Relations (blog), March 24, 2022. https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war.
[51] Monica Buchanan Pitrelli. "Anonymous Declared a 'Cyber War' Against Russia. Here Are the Results." CNBC.com, March 16, 2022, https://www.cnbc.com/2022/03/16/what-has-anonymous-done-to-russia-here-are-the-results-.html.
[52] Torey McMurdo. "Ukraine Has Been Winning the Messaging Wars. It's Been Preparing for Years." *Washington Post*, March 28, 2022.
[53] Stuart A. Thompson and Davey Alba, "In Ukraine's Information War, a Blend of Fact and Fiction," *The New York Times*, March 8, 2022, https://www.nytimes.com/2022/03/03/technology/ukraine-war-misinfo.html.