Military Cyber Affairs

Volume 4
Issue 2 *Technological Challenges in Cyberspace*

Article 1

December 2020

The Influence of Information Power Upon the Great Game in Cyberspace: U.S. Wins Over Russian Meddling in the 2018 Elections

Joseph H. Schafer
National Defense University, College of Information and Cyberspace, joseph.h.schafer.civ@msc.ndu.edu

The Influence of Information Power Upon the Great Game in Cyberspace: U.S. Wins Over Russian Meddling in the 2018 Elections

Erratum

Format corrections (various)

The Influence of Information Power Upon the Great Game in Cyberspace: U.S. Wins over Russian Meddling in the 2018 Elections[1]

Joseph H. Schafer

Abstract

The 2018 U.S. pivot in information[2] and cyberspace[3] degraded Russian operations in the 2018 election. Following pervasive Russian information power[4] operations during the U.S. 2016 elections, the United States progressed from a policy of preparations and defense in information and cyberspace[5] to a policy of forward engagement. U.S recognition of renewed great power competition coupled with Russia's inability to compete diplomatically, militarily (conventionally), or economically, inspires Russia to continues to concentrate on information power operations. This great game in cyberspace was virtually uncontested by the U.S. prior to 2017. Widespread awareness of Russian aggression in 2016 served as a catalyst which highlighted the enormity of Russian campaigns and the crippling constraints on U.S. information power. This catalyst pivoted the U.S. from a passive policy of preparations and defense in information and cyberspace to a policy of forward engagement that successfully attenuated Russian efforts in 2018.

By examining information power from theory development and Russian practice to recent reports and primary sources we find that the U.S. demonstrated the capability and willingness to defend forward successfully during the 2018 elections. Going forward, the U.S. must continue and expand efforts to contest cyberspace and counter disinformation to secure our democracy and the U.S. 2020 presidential election.

Introduction

The Central Intelligence Agency (CIA) National Intelligence Estimate Chairman wrote to the CIA director, 'This year', Moscow has 'made it plain that there are sharp distinctions between the contending parties and policies' and that the Kremlin has made 'their preference' known. The year was 1964. The Democratic candidate, Lyndon Johnson trounced his Republican opponent, Barry Goldwater overwhelmingly, as the Soviets had hoped. Twenty years later the CIA director was again warned and the Soviets 'unleashed the KGB's propaganda arm to paint Reagan as a militarist and warmonger, popularizing the slogan, 'Reagan Means War!" This information power campaign proved ineffectual as the Republican Ronald Reagan crushed the Democratic Walter Mondale in the 1984 election.[6]

The Soviets and the Russians have been attempting to influence[7] democratic elections in the U.S. and around the world for many, many years. More recently, following widespread Russian information power operations during the U.S. 2016 elections, the U.S. pivoted from a policy of preparations and defense in information and cyberspace to a policy of forward engagement. U.S recognition of renewed great power competition coupled with Russia's inability to compete diplomatically, militarily (conventionally), or economically, inspires Russia to continues to concentrate on information power operations. This great game in cyberspace was virtually uncontested by the U.S. prior to 2017. Widespread awareness of Russian efforts in 2016 served as a catalyst which highlighted the enormity of Russian campaigns and the crippling constraints on U.S. Information power. This catalyst pivoted the U.S. from a passive policy of preparations

and defense in information and cyberspace to a policy of forward engagement that successfully attenuated Russian efforts in 2018.

By examining information power from theory development and Russian practice to recent reports and primary sources we find that the U.S. demonstrated the capability and willingness to defend forward successfully during the 2018 elections. Going forward, the U.S. must continue and expand efforts to contest cyberspace and counter disinformation to secure our democracy and the U.S. 2020 presidential election.

Information Power Theory

The pivot represents a U.S. shift in policy and practice in the long-running debates on the nature and influences of information power. In many cultures and epochs, multidisciplinary practitioners and scholars have debated information power. 19th Century strategist and Prussian General Carl von Clausewitz wrote that "War . . . is an act of violence to compel our opponent to fulfill our will."[8] U.S military doctrine defines Informational Power as "the ability to affect behavior through the use of information."[9] The supremacy of information power has been acknowledged for centuries. Sun Tzu, the Chinese strategist, wrote 2,500 years ago, "To fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting."[10] An adversary's will is fulfilled without fighting, the enemy's resistance is broken, and their behavior affected by the power of information.

A near contemporary of Sun Tzu, Socrates lamented the development of writing which would provide information without proper instruction. The arrival of Gutenberg's printing press 2,000 years later spurred fears of intellectual laziness that would undermine authority. Many fears proved true and authorities were undermined, but the benefits of these informational technologies proved far more profound.[11] Ongoing concerns today about emerging technologies[12] highlight our continued tendency to both expect the best and the worst from information inventions.

Protecting and Defining Information power

The U.S. has recognized Information as an instrument of national power in the DIME construct (Diplomacy, Information, Military and Economics) for many years[13]. The U.S. has even recognized the need to protect information since 1775 when it established, in the Postal Service, the worlds' first government organization tasked with protecting citizen information.[14] Today's changes include multi-gigabit connectivity that is more than 300 million times faster than the telegraph and 30 billion times faster than the Pony Express.[15]

However, the U.S. has been slow to embrace the hybrid nature of information power particularly in response to population manipulation.[16] Researchers and practitioners have protested that information power is indispensable and yet has not garnered the attention of U.S. national security strategists, [17] until recently. From a theoretical perspective Claude Shannon's 1948 seminal information theory paper proved that information is a well-defined, measurable quantity[18] that can be treated like mass or energy[19] rather than an undefinable ether.[20] These laws physical laws establish the boundaries of information power. Politics shape cyberspace, as with writing and printing, as they shape land, sea, air, and space.[21] These boundaries are expanding as the vanishing cost the multiplying speed and reach of information power generates great promise and great vulnerability.

https://scholarcommons.usf.edu/mca/vol4/iss2/1
DOI: https://doi.org/10.5038/2378-0789.4.2.1076

Recognizing these vulnerabilities, state and non-state actors have been using information power, just as they would use more traditional powers and technologies to gain advantages. The U.S. military characterizes Information Operations (IO) as the integrated employment of information and cyberspace capabilities[22], "to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own."[23]

In addition to IO, the United States has used many phrases to describe the intersecting and overlapping concepts including Electronic, Information, Influence, Psychological, and Cyber Warfare. Despite doctrine for broader information operations, the U.S. paradigm of information power has concentrated on the information technology, telecommunications, and cyber infrastructure[24] even when the influence components have proven dominant. The information age remains unevenly distributed and the authority of states remain relevant. From the strategic perspective, the new synthetic domain of warfare is Cyberspace and the overarching phrase for national and military effects in information and cyberspace is Information Power.

Hard Power, Soft Power and Sharp Information power

A spectrum of power from coercive "Hard Power" to persuasive "Soft Power"[25] may describe all the diplomatic, information, military, and economic (DIME) elements of national power."[26] Hard and soft power can be applied by states for good or bad ends; soft power simply requires attractive and voluntary means.[27] Misleadingly, soft power has been used to describe all forms of influence and information power that are not hard military force. However, we observe many instantiations of influence which are not persuasive and this type of hard power that uses deceptive information for hostile ends is called "Sharp Power" to distinguish it from attractive soft power.[28] By design, distinguishing deceptive sharp power propaganda from open persuasive soft power can prove very difficult for nations and people. Much of the great game in cyberspace is played with sharp power.

The Great Game in Cyberspace

The "Great Game" refers to a 19th century period of competition between the British and Russian Empires in the 19th over influence in the Afghanistan region[29]. The Great Game primarily describes British responses to perceived Russian threats during this period of unclear motives, mistrust, intrigue, and malign influence[30]. The end of Cold War (1957-1991) period of competition between Soviet Union and the U.S. planted the seeds of renewed great power completion due to the economic, political, and alliance disruptions. Former Defense Secretary Robert Gates wrote in 2014 that, "No Russian was more angered by this turn of events than [Russian President] Vladimir Putin, who would later say that the end of the Soviet Union was the worst geopolitical event of the twentieth century."[31] A primary outlet for this anger is cyberspace.

Renewed Great Power Competition

Secretary of Defense Dr. Mark Esper has reiterated the observations of his predecessor[32], General Jim Mattis, U.S. Marine Corps (Retired), who wrote in the U.S. 2018 National Defense Strategy (NDS), "The central challenge to U.S. prosperity and security is the *reemergence of long-term, strategic competition* by what [President Trump's 2017] National Security Strategy classifies as revisionist powers."[33] Regarding Russia, Esper explicitly stated during his confirmation hearing on July 16, 2019, that we, "have entered a new era of great-power competition."[34]

"The Great Game in Cyberspace," coined here, is an apt if imperfect description of the current information power struggle below the level of kinetic armed military conflict with competitors including Russia. Although competitors have been spreading disinformation for millennia; a challenge in cyberspace is that attacks and their attribution can be more nuanced and more political than has been widely understood.[35] Though the attribution obstacles are diminishing, nowhere is the effect of these developments more far-reaching than on state sponsored information power operations.[36]

Wartime and Peacetime in Cyberspace

Democracies tend to draw sharp distinctions between the conditions and authorities of peacetime and wartime. Authoritarian regimes, less so, such that they develop integrated capabilities that operate across the conditions of international relationships."[37] However, despite actions and assertions to the contrary, aggression, even via information power in cyberspace, are not the normative behaviors of law-abiding nations.

From 2009 until 2012 law-abiding nations organized by NATO convened an international group of experts to document norms for operations in information and cyberspace. They published the *Tallinn Manual on the International Law Applicable to Cyber Warfare*, in 2013, [38] documenting relevant legal regimes in the cyber context. The focus was on cyber warfare "armed attacks" which allow states to respond in self-defense. A second and more diverse group of experts published *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* in 2017, which adds topics reflecting the reality of daily information and cyberspace "operations" that do not rise to the level of armed conflict.[39] Both manuals reflect "the law as it exists" according to international experts and describe the legal limits for operations in information and cyberspace.[40]

Since applicable international law remains unacknowledged by competitors, the game of great power competition has increasingly been played out in information and cyberspace. Russia increasingly engages in asymmetric attacks in information and cyberspace because the U.S. has far superior diplomatic, economic, and conventional military power.[41] U.S. recognition of renewed great power competition coupled with Russia's inability to compete diplomatically, militarily (conventionally), or economically, inspires Russia to continues to concentrate on information power operations.

Russian Information Power Operations

> ***"Foreign politicians talk about Russia's interference in elections and referendums around the world. In fact, the matter is even more serious: Russia interferes in your brains, we change your conscience, and there is nothing you can do about it."***
>
> – Vladislav Surkov, Adviser to Russian president Vladimir Putin[42]

The 2011 Russian Information Space Activities Concept states that Information War is the confrontation between states in the information space to 1) damage information systems, resources, and critical infrastructure, 2) undermine the political, economic and social systems, 3) massively manipulate populations to destabilize the state and society, and 4) coerce the states to make decisions for the benefit Russia.[43]

https://scholarcommons.usf.edu/mca/vol4/iss2/1
DOI: https://doi.org/10.5038/2378-0789.4.2.1076

Russia has proven particularly adept and active in manipulating information and cyberspace. "Russian propaganda entertains, confuses and overwhelms the audience."[44] It is often chaotic and dizzying.[45] Clausewitz reminds us that in contests between states, the political object is the ends or the goal, "war is the means of reaching it, and means can never be considered in isolation from their purpose."[46] Russian doctrine toward the means and ends of information power has focused on this asymmetric and hybrid approach. Through this hybrid warfare, Russia seeks to impose its will without crossing the threshold of armed conflict. "This insidious form of aggression includes military elements such as intelligence, cyber-attacks and fake news, as well as the firing of riots and terrorism. ... They are thus putting democracies at risk."[47]

Former Defense Secretary Mattis wrote in the 2018 DoD Cyber Strategy that: "Russia has used cyber-enabled information operations to influence our population and challenge our democratic processes."[48] The means of this campaign "include the use of deception, deflection of responsibility, outright lies, and the creation of an alternative reality."[49] Defense Secretary Esper recently stated that Russia has pursued and developed a very adept asymmetric capability in the realm of Information Warfare *"*because of the strength of our conventional forces."[50]

Russian Sharp Power

The current Russian approach to sharp power propaganda builds upon Soviet experiences and successes with obfuscation and motivating target actions without them realizing. However, it now leverages the evolving information environment in way unimaginable to their Soviet predecessors. This new Russian model has been called the "Firehose of Falsehood" because they rapidly and continuously leverage an enormous number of communications channels with a "shameless willingness to disseminate partial truths or outright fiction."[51]

The greatest successes of Soviet meddling or political warfare came from "fellow travelers whose agendas paralleled the Soviets' and who needed little if any coordination."[52]

Researchers have identified two waves of Russian meddling over the past twenty years. The first wave from demise of the Soviet Union in the early 1990s until 2014 targeted only post-Soviet countries. Since then, a second wave has expanded dramatically into established Western democracies including the recent French presidential elections, the Spanish Catalan independence poll, and the UK's BREXIT referendum, to cite a very few. "However, an examination of both of these waves shows that Russia's efforts have made little difference."[53]

Since 2014, researchers have provided empirical evidence on how Russia has moved towards a preference for Soviet-style active measures which blur of boundaries between public diplomacy, forgeries, disinformation, military threats, spys, and agents of influence. These sharp power active measures highlight Russian foreign policy strategy including goals for marginalizing NATO and democratic institutions around the world.[54]

Russian 2016 Election Interference and Workflow

Different in 2016 was the Russian intelligence success in influencing democratic elections and referenda by combining the traditional intelligence disciplines such as disinformation with cutting edge cyber tactics to create a hybrid intelligence, reminiscent of Soviet 'complex active measures'[55] Russia did not need to employ hard cyber-attacks such as hacking into voting machines, instead, the goals appear to have been to create mistrust about election results.[56] Despite vulnerabilities, "no allegations of altered vote tallies have surfaced, suggesting that the American people did get their intended result."[57]

Special Counsel, Robert Mueller's *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*, recapping a two year investigation, states that the Russian government backed "Internet Research Agency (IRA) carried out … a social media campaign designed to provoke and amplify political and social discord in the United States."[58] Indeed, the specified Russian goals of exacerbating American social polarization, continue mushrooming.

The Russian Internet Research Agency spent months creating fake American local news outlets; most stories were crafted to stir chaos and disgust towards candidates and issues.[59] The steps of the Russian fake news propaganda workflow include: 1. Create (or warp) an outrageous story. 2. Amplify the story in the traditional and social media. 3. Validate the story (i.e. with Russian leadership commentary) 4. Magnify the validated story with additional social buzz and shares 5. Propaganda are taken as fact by many people.[60] Fake news is one of the greatest threats to democracy, journalism, and economies because it has weakened public trust in governments and the institutions of democracy.[61]

In his opening statement, Mark Warner, Vice-Chair of the Senate Select Committee on intelligence noted the power of information operations in a networked world: "Russians have been conducting information warfare for decades. But what is new is the advent of social media tools with the power to magnify propaganda and fake news on a scale that was unimaginable back in the days of the Berlin Wall.[62]

Russia's broad social media presence can appear random. Indeed, all sides of polarizing issues have asserted that Russia is helping their opposition. However, the New York Times reports that Russia's information and cyberspace influence campaigns target content and audiences "cross all ideological boundaries."[63] Russian agents amplify divisive and emotionally outrageous messaging on all sides of any given issue, so much so that it sometimes appears as though the sole purpose of a disinformation operation is to sow general chaos in the targeted society.[64]

Emotionally outrageous fake news stories are 70% more likely to be retweeted and more rapidly. Because fake news is more sensational, it propagates further and faster than real news.[65] The reach of fake news was highlighted during the 2016 U.S. presidential election campaign. The top twenty fake election stories generated 8.7 million reactions comments on Facebook. Ironically, the top twenty election stories from major news websites generated only 7.4 million reactions.[66]

In late 2017, Facebook, Twitter, and Alphabet (Google) each provided enormous IRA data sets to the United States Senate Select Committee on Intelligence. Experts analyzed these text, images, videos, and other content data sets.[67] The magnitude of the IRA activities was immense, fueled by troll farms and fake news[68]—"reaching 126 million people on Facebook, posting 10.4 million tweets on Twitter, uploading 1,000+ videos to YouTube, and reaching over 20 million users on Instagram."[69] All intended to incite divisions in the U.S. electorate.

Black and Blue Lives: Russians Plan Both Sides

The Russian Internet Research Agency pursued "important internal problems" in the U.S. by creating a "media mirage" of social media pages and accounts within the target community[70]. African Americans were relentlessly targeted. According to Senate Intelligence Committee reports, an individual that followed a single IRA account, "would have been exposed to content from dozens more, as well as carefully-curated authentic Black media content that was ideologically or thematically aligned."[71]

https://scholarcommons.usf.edu/mca/vol4/iss2/1
DOI: https://doi.org/10.5038/2378-0789.4.2.1076

For instance, #BlackLivesMatter is an authentic movement. Russians duped citizens with inauthentic Twitter and Facebook accounts to inflame opinions about police shootings to reinforce a narrative that the justice system was deeply racist.[72] Seeking to further incite divisions, the Russians hijacked the murder of five police officers on July 7 2016 and exploded the divide by viralizing the counter-movement, #BlueLivesMatter.[73] The IRA's inauthentic communities on both sides "pulled users into a virtual vortex; ... doubly dangerous because the content was often based on kernels of truth."[74] Playing both sides, Russia aggressively propagandized citizens so that advocating or criticizing police officers became politicized.[75]

Russian Goals

> ***"Russian efforts to influence the 2016 U.S. presidential election represent the most recent expression of Moscow's longstanding desire to undermine the U.S.-led liberal democratic order, but these activities demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations."***[76]
>
> James R. Clapper, Director of National Intelligence (DNI), January 6, 2017

Broader than simply inciting divisions in the U.S. electorate, weakening the Western global order is a primary Russian strategy directly inherited from the Cold War Soviets. Russia intensifies hyperpartisanship and extreme movements. Russia relies heavily on information and cyberspace attacks on the U.S. and NATO allies to stoke divisions and undercut confidence in politics and civil society.[77]

Director Clapper's report goes on to say that Russian President Vladimir Putin ordered information power campaign against the 2016 U.S. presidential election. Russia's goals were to undermine public faith in the U.S. democratic process and denigrate Secretary Clinton.[78] Putin has publicly blamed Clinton since 2011 for inciting protests against his regime at that time for disparaging comments she made against him.[79] Many researchers agree that Hillary Clinton's "criticism of Putin infuriated him and served as a key motivator for the Kremlin's meddling in the U.S. election of 2016."[80]

In addition to police issues, substantial content was Pro-Sanders, Pro-Trump, and Anti-Clinton. The IRA targeted many major divides including fake communities that supported and opposed Christians, Muslims, LGBT, feminists, immigrants, and refugees.[81] These Russian information and cyberspace sharp power attacks hamper civil discourse because they degrade rather than persuade across the spectrum of shared and political common-knowledge.[82]

In May 2017, Former CIA and National Security Agency director General Michael Hayden described Russian meddling in the 2016 U.S. Presidential election as "the most successful covert influence campaign in history"[83] A month later, now former DNI Clapper summed up goals and effects in Senate testimony, The Russians "must be congratulating themselves for having exceeded their wildest expectations with a minimal expenditure of resources'.[84] This great game in cyberspace was virtually uncontested by the U.S. prior to 2017.

U.S. Information and Cyberspace Policy History and 2018 Pivot

Following pervasive Russian information power operations during the U.S. 2016 elections, the U.S. progressed from a policy of preparations and defense in information and cyberspace to a

policy of forward engagement. Widespread awareness of Russian aggression in 2016 served as a catalyst which highlighted the enormity of Russian campaigns and the crippling constraints on U.S. Information power. This catalyst pivoted the U.S. from a passive policy of preparations and defense in information and cyberspace to a policy of forward. This blatant meddling in 2016 spurred U.S. preparations and policies that successfully attenuated Russian aggression in 2018.

Early U.S. Information and Cyberspace Policy

In February 2003, three months after consolidating 22 U.S. agencies into the Department of Homeland Security (DHS), President George W. Bush released the first U.S. National Strategy to Secure Cyberspace.

U.S. Department of Defense information and cyberspace organizations continued to mature during this period through a number of Joint Task Forces aligned with the Defense Information Systems Agency (DISA) and the National Security Agency (NSA) culminating with the creation of the U.S. Cyber Command (USCYBERCOM) as a subunified command of the U.S. Strategic Command in 2009.[85]

Policies Prior to the U.S. 2016 Elections

General Keith Alexander, nominated in 2010 by President Barack Obama as the first commander of the new U.S. Cyber Command (USCYBERCOM), stated during his confirmation hearing that there was a "mismatch between our technical capabilities to conduct operations and the governing laws and policies."[86] USCYBERCOM continued its initial focus on technical capabilities, defense, and response.

In May 2011, President Barack Obama's "International Strategy for Cyberspace" stated: "When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners. … —as appropriate and consistent with applicable international law, … we will exhaust all options before military force whenever we can;… seeking broad international support whenever possible."[87] **Russia was not mentioned at all.**

The Strategic Goals of the Obama Administration's 2015 DoD Cyber Strategy describes defending DoD missions and U.S. interests.[88] "The United States will continue to respond to cyberattacks against U.S. interests at a time, in a manner, and in a place of our choosing, using appropriate instruments of U.S. power and in accordance with applicable law."[89] Noting that "Russian actors are stealthy in their cyber tradecraft and their intentions are sometimes difficult to discern."[90]

In May 2017, USCYBERCOM Commander Admiral Mike Rogers submitted testimony to the House Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities on the "Cyber Threat Environment." 25% of the eleven page assessment was devoted to ISIS terrorist influence campaigns and much of the remaining described threats to information systems.[91] A single sentence to mentions concern for "states seeking to shape the policies and attitudes of democratic peoples" **again with no mention of Russian influence campaigns**.[92]

As with nuclear weapons, President Obama had sole authority to authorize the use of cyberweapons in recognition that they could can have mass destruction effects.[93] However,

https://scholarcommons.usf.edu/mca/vol4/iss2/1
DOI: https://doi.org/10.5038/2378-0789.4.2.1076

deterrence in cyberspace is much different than nuclear deterrence. Nuclear deterrence total prevention due to fears of mutually assured destruction. In contrast, information and cyber effects are continuous.[94]

Aside from failing to acknowledge the Russian aggression in information and cyberspace, the most challenging problem for Obama – as expressed by "Democrats and Republicans with vast experience in national security" is his "micromanagement of the Pentagon and Intelligence Community by a bloated and lackluster National Security Council." In fact, after leaving the Pentagon, "Obama's first three secretaries of Defense — Robert M. Gates, Leon E. Panetta and Chuck Hagel — accused the Obama White House of micromanaging the military."[95]

Policy Pivot Prior to the 2018 Election

Frustration with the unremitting defeats in information and cyberspace drove a series of bipartisan legislative and executive remedies. In a dramatic shift, President Donald Trump's 2017 National Security Strategy[96] labels Russia's actions in cyberspace as "destabilizing" and asserts that Russia "uses information operations as part of its offensive cyber efforts to influence public opinion across the globe. Through modernized forms of subversive tactics, Russia interferes in the domestic political affairs of countries around the world."[97]

The U.S. military emphasis on information and cyberspace has soared in the past few months with 1) the recognition that Cyberspace is the fifth domain of warfare (alongside Land, Sea, Air, and Space), 2) the promotion of the U.S. Cyber Command to Combatant Command status, and 3) most recently the elevation of Information as the seventh joint function (The Joint Functions are: C2, intelligence, fires, movement and maneuver, protection, sustainment, and information.).[98]

Defense Secretary James Mattis endorsed the introduction of *Information* as a new, seventh joint function signaling[99] "a fundamental appreciation for the military role of information at the strategic, operational and tactical levels within today's complex operating environment."[100] Additionally, the Defense Authorization Act of 2017, re-designated the National Defens University's Information and Resource Management College (IRMC) as the College of Information and cyberspace (CIC).[101] And on 4 May 2018 the U.S. Cyber Command was elevated to Unified Combatant Command status, raising its stature as a direct report to the Secretary of Defense. The elevation reinforces the importance of information and cyberspace, reassure allies, deters adversaries, and streamlines control of time sensitive operations.[102]

President Trump's 2018 National Cyber Strategy asserts that "The United States will use all appropriate tools of national power to expose and counter the flood of online malign influence and information campaigns and non-state propaganda and disinformation."[103]

The 2018 National Defense Strategy goes on to emphasize that Russia is competing across all dimensions of power and seeks to shatter NATO and to shape an authoritarian world with control over other nations' structures and decisions. Specifically, Russia has "increased efforts short of armed conflict by expanding coercion to new fronts, violating principles of sovereignty, exploiting ambiguity, and deliberately blurring the lines between civil and military goals."[104]

Secretary Mattis further asserts in the 2018 U.S. Defense Cyber Strategy that "Russia has used cyber-enabled information operations to influence our population and challenge our democratic processes. … We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict."[105] The 2018 cyberspace objectives include ensuring the US military can achieve objectives contested cyberspace, conducting cyber

operations to enhance U.S. military advantages, defending U.S. and DoD (including civilian assets that enable military advantage) from cyber-attacks that could be significant, and expanding cooperation with interagency, industry, and international partners.[106]

In September 2018 President Trump signed Executive Order 13848 enabling sanctions for foreign interference that attempts to "influence, undermine confidence in, or alter the result or reported result" of an election or "undermine public confidence in election processes or institutions."[107]

The 2016 election interference catalyst pivoted the U.S. from the passive policy of defense in information and cyberspace to a policy of engagement to defend forward for the 2018 elections. These changes were lauded by many, across the political spectrum, such as Democratic Congressmen James Langevin, Co-Chair of the House Cybersecurity Caucus, who spoke of bipartisan support for the new approach during a keynote address in Washington.[108] However, this more active posture was met with substantial criticism as well including media assertions such as: "Under the Trump administration, the traditional structure of White House oversight of American offensive and defensive cyber activities is being dismantled."[109]

USCYBERCOM Defending Forward

> ***Russia has used cyber-enabled information operations to influence our population and challenge our democratic processes. … USCYBERCOM has recently improved the scope, speed, and effectiveness of its operations with the help of legal and policy changes.***[110]
>
> USCYBERCOM Commander and NSA Director, General Paul Nakasone
> Testimony to the U.S. Senate Armed Service Committee

These changes in policy from response to persistent engagement aligned USCYBERCOM with the 2017 National Security Strategy and the 2018 National Defense Strategy which each highlight the return of great power competition – particularly as it is shifted towards cyberspace and below the level of armed conflict.[111]

General Nakasone, the Commander of USCYBERCOM and the Director of the National Security Agency explained in a recent interview that, we must keep in mind four foundations concepts in cyberspace: 1) we are in constant contact with adversaries, 2) our security is challenged, 3) superiority is ephemeral, and 4) advantage favors initiative. Thus, the cyber domain is one of constant action to defend actively, to conduct reconnaissance, to understand capabilities and intent, and to improve quickly.[112]

In a recent article, General Nakasone elaborates: "We must "defend forward" in cyberspace, as we do in the physical domains. Our naval forces do not defend by staying in port, and our airpower does not remain at airfields. They patrol the seas and skies to ensure they are positioned to defend our country before our borders are crossed. The same logic applies in cyberspace."[113] We cannot succeed if we stay inside our own networks. "Shifting from a response outlook to a persistence force that defends forward moves our cyber capabilities out of their virtual garrisons, adopting a posture that matches the cyberspace operational environment."[114]

https://scholarcommons.usf.edu/mca/vol4/iss2/1
DOI: https://doi.org/10.5038/2378-0789.4.2.1076

USCYBERCOM's Number One Priority in 2018

> ***"Ensuring a safe and secure election was our No. 1 priority, and drove me to establish a joint U.S. Cyber Command/NSA effort we called the Russia Small Group."***[115]
>
> USCYBERCOM Commander and NSA Director, General Paul Nakasone
> Testimony to the Senate Armed Service Committee

General Nakasone went on to tell lawmakers that protecting the 2018 midterms from meddling adversaries was both a priority and a challenge. "In the last 10 years, our adversaries have been operating below the threshold of armed conflict, stealing our intellectual property, leveraging our personally identifiable information, or attempting to influence our elections." This is why USCYBERCOM "evolved its strategic concept and operational approach from a response force to a persistence force."[116]

Defense Secretary Esper expounded on the final enabling order during his confirmation hearing. Secretary Esper credited the 2018 National Security Presidential Memorandum (NSPM) 13 as being just as important as our great capabilities because is allowed our cyber forces to "lean forward" into a more offensive posture. NSPM-13 replaced the previous process which required presidential approval for cyber operations. The new policy allows the president to delegate authorities. Esper credited NSPM-13 with unleashing the great capability of U.S. Cyber Command to secure the 2018 elections.[117]

Again, with this approach, comes risks. Media reported that, "The Pentagon has quietly empowered the United States Cyber Command to take a far more aggressive approach to defending the nation against cyberattacks, a shift in strategy that could increase the risk of conflict with the foreign states that sponsor malicious hacking groups." [118]

U.S. Information Power Results and Implications

By examining information power from theory development and Russian practice to recent reports and primary sources we find that the U.S. demonstrated the capability and willingness to defend forward successfully during the 2018 elections.

USCYBERCOM struck the Russian Internet Research Agency during the 2018 midterms took them offline as part of "the first offensive cyber campaign against Russia designed to thwart attempts to interfere with a U.S. election." [119] This was the first operation by USCYBERCOM, "with intelligence from the National Security Agency, under new authorities it was granted by President Donald Trump and Congress last year to bolster offensive capabilities."[120]

Despite our success during the 2018 elections, the mission of defending our nation in information and cyberspace remains "one of the least developed mission areas and one in which there is little consensus on what it means to defend the nation and its interests in cyberspace, or on what role the Department of Defense should be for this mission."[121]

Secretary Esper further stated during his confirmation hearing that, "We are at war in the cyber domain now battling countries like Russia and China who are doing everything from stealing technology to influencing elections to putting out disinformation about the United States."[122] Having demonstrated the capability and willingness to defend forward, the U.S. must continue,

clarify, and expand efforts to contest cyberspace and counter disinformation to secure our democracy and the U.S. 2020 presidential election.

Biography

Joseph H. Schafer is Professor and Chair of the Leadership and Strategy Department and Director of the Leadership Development Program for the College of Information and cyberspace at the National Defense University. He is a graduate of the Army Command and General Staff College and the Defense Systems Management College. Dr. Schafer has served on the faculty at George Washington University, West Point, and the Defense Acquisition University and has held executive roles at L-3 and Dell. Joseph has a BS in Electrical Engineering and Computer Science from West Point, MS in Computer Science / Artificial Intelligence and PhD in Computer Science / Cybersecurity from GW, MA in Strategy from the Naval War College, and an MBA from the UVA Darden School. He has lectured widely and his current research focuses on influence and emerging technology applied to security and strategy.

https://scholarcommons.usf.edu/mca/vol4/iss2/1
DOI: https://doi.org/10.5038/2378-0789.4.2.1076

Endnotes

[1] The views and ideas expressed here are the authors alone and do not represent those of the U.S. Government, the U.S. Department of Defense, or U.S. National Defense University (NDU) College of Information and cyberspace (CIC).

[2] Daniel T Kuehl, "Chapter 1: Introduction: Brother, Can You Spare Me a DIME," in *Information Warfare: Separating Hype from Reality*, ed. E. Leigh Armistead (Washington, DC: Potomac Books, 2007), 4. Information is the message and understanding in people.

[3] JCS, *DOD Dictionary of Military and Associated Terms* (Washington, DC: Joint Chiefs of Staff, June 2019), 57, https://www.jcs.mil/Doctrine/DOD-Terminology/. Cyberspace is the information infrastructure and is the fifth domain of warfare alongside Land, Sea, Air, and Space; the only synthetic warfare domain.

[4] E. Leigh Armistead, ed., *Information Operations: Warfare and the Hard Reality of Soft Power*, 1 edition (Washington, DC: Potomac Books, 2004), 10. "Power is defined as 'the ability of A to get B to do something that B would not otherwise do.'"

[5] John B. Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War," *Strategic Studies Quarterly. Air University*, Summer 2011, 96.

[6] David V. Gioe, "Cyber Operations and Useful Fools: The Approach of Russian Hybrid Intelligence," *Intelligence and National Security* 33, no. 7 (November 10, 2018): 954–55, https://doi.org/10/gf5jjw.

[7] "Definition of INFLUENCE," https://www.merriam-webster.com/dictionary/influence. "the power or capacity of causing an effect in indirect or intangible ways"

[8] Carl von Clausewitz, *On War*, ed. Peter Paret, trans. Michael Howard (Princeton, NJ: Princeton University Press, 1976), 90.

[9] JCS, *Joint Publication 3-XX, Information (Final Coordination DRAFT)* (The Pentagon: The Joint Staff, TBP 2019), 14; Draft JP3-xx is expected to replace JP3-13, "Information Operations". JP3-12, "Cyberspace Operations" is expected to remain. JCS, *Joint Publication 3-13: Information Operations* (The Pentagon: The Joint Staff, November 27, 2012), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf; JCS, *Joint Publication 3-12: Cyberspace Operations* (The Pentagon: The Joint Staff, June 8, 2018), https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series/.

[10] Sun Tzu, *On the Art of War*, trans. Lionel Giles (London: The British Museum, 1910), 17.

[11] Nicholas Carr, "Is Google Making Us Stupid?," The Atlantic, July 1, 2008, https://www.theatlantic.com/magazine/archive/2008/07/is-google-making-us-stupid/306868/.

[12] Relevant emerging technologies include artificial intelligence, 5G, machine learning, quantum computing, etc.

[13] DIME: Diplomacy, Information, Military and Economics per Office of the Chairman of the Joint Chiefs of Staff, *JP 1, Doctrine for the Armed Forces of the United States* (Washington, DC: The Joint Staff, March 25, 2013), I-12-I–14, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf.

[14] "History of The United States Postal Inspection Service | USPIS," *United States Postal Inspection Service* (blog), https://www.uspis.gov/about/history-of-uspis/. USPIS is also the oldest U.S. Federal law enforcement agency (and originator of the term 'special agent').

[15] Tom Wheeler, "Connections Have Consequences," in *From Gutenberg to Google: The History of Our Future* (Washington, DC: Brookings Institution Press, 2019), 22, https://www.brookings.edu/wp-content/uploads/2018/02/9780815735328_ch1.pdf.

[16] Nick Brunetti-Lihach, "Information Warfare Past, Present, and Future," *The Strategy Bridge*, November 14, 2018, https://thestrategybridge.org/the-bridge/2018/11/14/information-warfare-past-present-and-future.

[17] Dennis M. Murphy and Daniel T Kuehl, "The Case for a National Information Strategy," October 2015, 72.

[18] Claude Elwood Shannon, "A Mathematical Theory of Communication," *The Bell System Technical Journal*, American Telephone & Telegraph Co., 27 (October 1948): 379–423, 623–56, https://doi.org/10/b39t.

[19] Claude Elwood Shannon, *Development of Communication and Computing, and My Hobby*, Presentation (Kyoto, Japan: Kyoto Prize, Inamori Foundation, November 12, 1985), https://www.kyotoprize.org/en/laureates/claude_elwood_shannon/.

[20] James V. Stone, "Information Theory: A Tutorial Introduction," *ArXiv:1802.05968 [Cs, Math, Stat]*, February 16, 2018, 1.

[21] Robert O. Keohane and Joseph S. Nye, "Power and Interdependence in the Information Age," *Foreign Affairs* 77, no. 5 (1998): 82–85, https://doi.org/10/bz6g6v.

[22] JCS, *JP 3-13*, I–3. "The employment of [Information Related Capabilities] IRCs is complemented by a set of capabilities such as operations security (OPSEC), information assurance (IA), counterdeception, physical security, electronic warfare (EW) support, and electronic protection. These capabilities are critical to enabling and protecting the [Joint Force Commander's] JFC's [Command and Control] C2 of forces." Additional capabilities such as computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC) have also been related to information operations.

[23] JCS, ix. The Glossary of JP3-13 defines Information Operations as "The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. Also called IO."

[24] Daniel T. Kuehl, *Defining Information Power*, Strategic Forum (Washington, DC: National Defense University, June 1997), 5, https://apps.dtic.mil/docs/citations/ADA394366.

[25] Joseph Samuel Nye Jr., *Soft Power: The Means to Success in World Politics*, vol. 1st ed (New York: Public Affairs, 2004).

[26] Joseph Samuel Nye Jr., "The Future of Power," Belfer Center for Science and International Affairs, February 2011, 21, https://www.belfercenter.org/publication/future-power-0.

[27] Joseph Samuel Nye Jr., "How Sharp Power Threatens Soft Power," *Foreign Affairs*, January 2, 2019, http://www.foreignaffairs.com/articles/china/2018-01-24/how-sharp-power-threatens-soft-power.

[28] Christopher Walker and Jessica Ludwig, "From 'Soft Power' to 'Sharp Power': Rising Authoritarian Influence in the Democratic World," in *"Sharp Power": Rising Authoritarian Influence*, ed. Christopher Walker, Jessica Ludwig, and Shanthi Kalathil (Washington, DC: The International Forum for Democratic Studies at the National Endowment for Democracy, 2017), 13, https://www.ned.org/events/sharp-power-rising-authoritarian-influence/.

[29] The Great Game was a confrontation between the Russian and British Empires in the 1800s. Used here as an analogy. See: Edward Ingram, "Great Britain's Great Game: An Introduction," *The International History Review* 2, no. 2 (April 1980): 160–71, https://doi.org/10/cj3ztf.

[30] Barbara Jelavich, *St. Petersburg and Moscow: Tsarist and Soviet Foreign Policy, 1814-1974*, First Edition edition (Bloomington: Indiana University Press, 1974), 200.

[31] Robert M. Gates, *Duty: Memoirs of a Secretary at War* (New York: Knopf, 2014), 149–50.

[32] Richard Sisk, "Esper Pledges 'Tough Decisions' on China, Russia If Confirmed as Defense Secretary," Military.com, July 16, 2019, https://www.military.com/daily-news/2019/07/16/esper-pledges-tough-decisions-china-russia-if-confirmed-defense-secretary.html.

[33] James Norman Mattis, *Summary of the 2018 National Defense Strategy of the United States of America*, January 1, 2018, https://www.hsdl.org/?abstract&did=.

https://scholarcommons.usf.edu/mca/vol4/iss2/1
DOI: https://doi.org/10.5038/2378-0789.4.2.1076

[34] RM Staff, "Esper on Russia: Pentagon Nominee Sees Moscow as 'Strategic Competitor,' 'Potential Adversary,'" *Russia Matters. Harvard Kennedy School's Belfer Center for Science and International Affairs*, July 17, 2019, https://www.russiamatters.org/analysis/esper-russia-pentagon-nominee-sees-moscow-strategic-competitor-potential-adversary.

[35] Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1–2 (January 2, 2015): 6, https://doi.org/10/ckvx.

[36] David Jablonsky, "National Power," *Parameters, U.S. Army War College Quarterly*, Spring 1997, 34–54.

[37] Herbert Lin and Jaclyn Kerr, "On Cyber-Enabled Information Warfare and Information Operations," in *Oxford Handbook of Cybersecurity*, 2019, 29.

[38] Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Reprint edition, NATO Cooperative Cyber Defence Centre of Excellence (Cambridge; New York: Cambridge University Press, 2013).

[39] Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd Edition (Cambridge, United Kingdom; New York, NY, USA: Cambridge University Press, 2017), https://ccdcoe.org/research/tallinn-manual/.

[40] Eric Talbot Jensen, "The Tallinn Manual 2.0: Highlights and Insights," *Georgetown Journal of International Law* 48 (2017): 738.

[41] Lin and Kerr, "On Cyber-Enabled Information Warfare and Information Operations," 2.

[42] Steven Erlanger, "Russia's RT Network: Is It More BBC or K.G.B.? - The New York Times," *New York Times*, March 8, 2017, https://www.nytimes.com/2017/03/08/world/europe/russias-rt-network-is-it-more-bbc-or-kgb.html.

[43] Russian MoD, *Russian Federation Armed Forces' Information Space Activities Concept* (Moscow: Russian Ministry of Defense, 2011), http://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle.

[44] Giorgio Bertolin, "Conceptualizing Russian Information Operations: Info-War and Infiltration in the Context of Hybrid Warfare," *IO Sphere: The Professional Journal of Joint Information Operations*, Summer 2015, 10.

[45] Erlanger, "Russia's RT Network: Is It More BBC or K.G.B.? - The New York Times."

[46] Clausewitz, *On War*, 87.

[47] Ralph D. Thiele, *Democracy Under Fire*, ISPSW Strategy Series: Focus on Defense and International Security (Berlin: Institute for Strategic, Political, Security and Economic Consultancy (ISPSW), June 2019), 2, https://www.hsdl.org/?abstract&did=826765.

[48] James Norman Mattis, *Summary: 2018 Department of Defense Cyber Strategy* (The Pentagon: Department of Defense, January 2018), 1.

[49] Timothy Thomas, "Russia's 21st Century Information War: Working to Undermine and Destabilize Populations," *Defence Strategic Communications* 1, no. 1 (December 31, 2015): 11, https://doi.org/10/gf5gzv.

[50] RM Staff, "Esper on Russia: Pentagon Nominee Sees Moscow as 'Strategic Competitor,' 'Potential Adversary.'"

[51] Christopher Paul and Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It*, 2016, 1, https://www.rand.org/pubs/perspectives/PE198.html.

[52] Angelo Codevilla, "Political Warfare: A Set of Means for Achieving Political Ends," in *Strategic Influence: Public Diplomacy, Counterpropaganda, and Political Warfare* (Washington, DC: Institute of World Politics Press, 2009), 216, http://it4sec.org/article/political-warfare-means-achieving-political-ends.

[53] Lucan Ahmad Way and Adam Casey, "Russia Has Been Meddling in Foreign Elections for Decades. Has It Made a Difference?," *Washington Post*, January 8, 2018, sec. Monkey Cage Analysis,

https://www.washingtonpost.com/news/monkey-cage/wp/2018/01/05/russia-has-been-meddling-in-foreign-elections-for-decades-has-it-made-a-difference/.

[54] Martin Kragh and Sebastian Åsberg, "Russia's Strategy for Influence through Public Diplomacy and Active Measures: The Swedish Case," *Journal of Strategic Studies* 40, no. 6 (September 19, 2017): 773–816, https://doi.org/10/gcz9f2.

[55] Gioe, "Cyber Operations and Useful Fools," 954.

[56] Joseph Samuel Nye Jr., *Protecting Democracy in an Era of Cyber Information War* (Harvard Kennedy School: Belfer Center for Science and International Affairs, February 2019), 9, https://www.belfercenter.org/publication/protecting-democracy-era-cyber-information-war.

[57] Gioe, "Cyber Operations and Useful Fools," 957.

[58] Robert S. Mueller, *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*, The Mueller Report, Special Counsel, March 1, 2019, 4, https://www.hsdl.org/?abstract&did=.

[59] Nye Jr., *Protecting Democracy in an Era of Cyber Information War*, 11.

[60] Oz Sultan, "Tackling Disinformation, Online Terrorism, and Cyber Risks into the 20," *The Cyber Defense Review*, Spring 2019, 45.

[61] Xinyi Zhou et al., "Fake News: Fundamental Theories, Detection Strategies and Challenges," in *Proceedings of the Twelfth ACM International Conference on Web Search and Data Mining - WSDM '19* (the Twelfth ACM International Conference, Melbourne VIC, Australia: ACM Press, 2019), 836–37, https://doi.org/10/gf2nsw.

[62] "Social Media Influence in the 2016 U.S. Election," § Intelligence Committee (2017), 10, https://www.intelligence.senate.gov/hearings/open-hearing-social-media-influence-2016-us-elections.

[63] Jim Rutenberg, "RT, Sputnik and Russia's New Theory of War - The New York Times," *New York Times Magazine*, September 13, 2017, https://www.nytimes.com/2017/09/13/magazine/rt-sputnik-and-russias-new-theory-of-war.html.

[64] Suzanne Spaulding, Devi Nair, and Arthur Nelson, *Beyond the Ballot: How the Kremlin Works to Undermine the U.S. Justice System*, CSIS Defending Democratic Institutions Project (Washington, DC: Center for Strategic and International Studies (CSIS), May 2019), 19, https://www.csis.org/analysis/beyond-ballot-how-kremlin-works-undermine-us-justice-system.

[65] Nye Jr., *Protecting Democracy in an Era of Cyber Information War*, 11.

[66] Craig Silverman, "This Analysis Shows How Viral Fake Election News Stories Outperformed Real News On Facebook," *BuzzFeed News* (blog), November 16, 2016, https://www.buzzfeednews.com/article/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook.

[67] Renee DiResta et al., *The Tactics & Tropes of the Internet Research Agency* (Austin, TX: NewKnowledge, July 26, 2018), 2, https://www.newknowledge.com/articles/the-disinformation-report/.

[68] Neil MacFarquhar, "Inside the Russian Troll Factory: Zombies and a Breakneck Pace," *The New York Times*, February 18, 2018, sec. World, https://www.nytimes.com/2018/02/18/world/europe/russia-troll-factory.html.

[69] Renee DiResta, "Disinformation Report Slides Presentation on the Russian Internet Research Agency Content Analysis," § Senate Select Committee on Intelligence (2018), 2, https://disinformationreport.blob.core.windows.net/disinformation-report/NewKnowledge-Disinformation-Report-Slides.pdf.

[70] DiResta, Disinformation Report Slides Presentation on the Russian Internet Research Agency Content Analysis.

[71] Renee DiResta, "Statement by the Director of Research of NewKnowlege on the Russian Internet Research Agency Content Analysis," § Senate Select Committee on Intelligence (2018),

https://scholarcommons.usf.edu/mca/vol4/iss2/1
DOI: https://doi.org/10.5038/2378-0789.4.2.1076

https://www.intelligence.senate.gov/hearings/open-hearing-foreign-influence-operations%E2%80%99-use-social-media-platforms-third-party-expert.

[72] Spaulding, Nair, and Nelson, *Beyond the Ballot*, 24.

[73] Spaulding, Nair, and Nelson, 24.

[74] DiResta et al., *The Tactics & Tropes of the Internet Research Agency*.

[75] Spaulding, Nair, and Nelson, *Beyond the Ballot*, 25.

[76] James R Clapper, *Background to "Assessing Russian Activities and Intentions in Recent U.S. Elections": The Analytic Process and Cyber Incident Attribution*, January 6, 2017, 7, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[77] Steven Metz, "How Russia Crafted a Three-Dimensional Strategy to Regain Global Influence," *World Politics Review*, April 27, 2018, 1–3.

[78] Clapper, *Background to "Assessing Russian Activities and Intentions in Recent U.S. Elections": The Analytic Process and Cyber Incident Attribution*, 7.

[79] Clapper, 11.

[80] James P Farwell, "Countering Russian Meddling in U.S. Political Processes," *Parameters, U.S. Army War College Quarterly* 48, no. 1 (Spring 2018): 44.

[81] DiResta et al., *The Tactics & Tropes of the Internet Research Agency*, 11.

[82] Henry Farrell and Bruce Schneier, *Common-Knowledge Attacks on Democracy*, SSRN Scholarly Paper (Harvard University: The Berkman Klein Center for Internet & Society Research, October 1, 2018), 4, https://cyber.harvard.edu/story/2018-10/common-knowledge-attacks-democracy.

[83] Gen Michael Hayden, "Michael Hayden: U.S. Intel Agencies Win Big, but Russia Intel Wins Bigger in Comey Hearing," Text, *TheHill* (blog), March 22, 2017, https://thehill.com/blogs/pundits-blog/the-administration/325250-michael-hayden-us-intel-agencies-win-big-but-russia.

[84] James R Clapper, "Statement of James R. Clapper, Former Director of National Intelligence, Concerning Russian Interference in the 2016 United States Election," § Committee on the Judiciary Subcommittee on Crime and Terrorism (2017), https://www.judiciary.senate.gov/imo/media/doc/05-08-17%20Clapper%20Testimony.pdf.

[85] USCC, "U.S. Cyber Command History," https://www.cybercom.mil/About/History/. "President Donald J. Trump announced Aug. 18, 2017, his decision to accept Defense Secretary James Mattis' recommendation to elevate USCYBERCOM from a sub-unified command under USSTRATCOM to a Unified Combatant Command responsible for cyberspace operations. The decision to elevate USCYBERCOM was seen as a recognition of the growing centrality of cyberspace to U.S. national security and an acknowledgment of the changing nature of warfare. USCYBERCOM became a CCMD May 4, 2018, during the combined Change of Command/Change of Directorship ceremony at the new Integrated Cyber Center/Joint Operations Center (ICC/JOC) located at Fort Meade."

[86] Thom Shanker, "Cyberwar Nominee Sees Gaps in Law," *The New York Times*, April 14, 2010, sec. World, https://www.nytimes.com/2010/04/15/world/15military.html.

[87] Barack Hussein Obama II, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World [2011]* (Washington, DC: The White House, May 2011), 14.

[88] Ash Carter, *Department of Defense Cyber Strategy [2015]* (The Pentagon: Department of Defense, April 2015), 13–15.

[89] Carter, 11.

[90] Carter, 9.

[91] Michael S. Rogers, "Statement of the Commander, United States Cyber Command during Fiscal Year 2018 Budget Request for U.S. Cyber Command: Cyber Mission Force Support to Department of Defense Operations," § Subcommittee on Emerging Threats and Capabilities (Committee on Armed Services) (2017), https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=105988.

[92] Cathy Downes, "Strategic Blind-Spots on Cyber Threats, Vectors and Campaigns," *Cyber Defense Review* 3, no. 1 (Spring 2018): 100.

[93] David E. Sanger, "Pentagon Puts Cyberwarriors on the Offensive, Increasing the Risk of Conflict," *The New York Times*, June 17, 2018, sec. U.S., https://www.nytimes.com/2018/06/17/us/politics/cyber-command-trump.html.

[94] Nye Jr., *Protecting Democracy in an Era of Cyber Information War*, 16.

[95] Christi Parsons and W. J. Hennigan, "President Obama, Who Hoped to Sow Peace, Instead Led the Nation in War," www.latimes.com, http://www.latimes.com/projects/la-na-pol-obama-at-war/.

[96] Donald John Trump, *National Security Strategy of the United States of America [2017]* (Washington, DC: The White House, December 2017).

[97] Michael Sulmeyer, "Cybersecurity in the 2017 National Security Strategy," *Lawfare: Hard National Security Choices* (blog), December 19, 2017, https://www.lawfareblog.com/cybersecurity-2017-national-security-strategy.

[98] "Functions common to joint operations at all levels of warfare fall into seven basic groups—C2, information, intelligence, fires, movement and maneuver, protection, and sustainment. Some functions, such as C2, information, and intelligence, apply to all operations." Office of the Chairman of the Joint Chiefs of Staff, *JP 3-0, Joint Operations* (Washington, DC: The Joint Staff, January 17, 2017), III–1, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf.

[99] MAJ Josh Darling, "Information as a Joint Function A Doctrinal Perspective" (December 7, 2017).

[100] James Norman Mattis, "Information as a Joint Function. SECDEF Endorsement Memorandum" (U.S. Secretary of Defense, September 15, 2017).

[101] CIC, "Officially the College of Information and Cyberspace," College of Information and Cyberspace, June 14, 2017, http://icollege.ndu.edu/NEWS/News-Announcements/Article/1213612/officially-the-college-of-information-and-cyberspace/.

[102] Lisa Ferdinando, "Cybercom to Elevate to Combatant Command," U.S. Department of Defense News, May 3, 2018, https://dod.defense.gov/News/Article/Article/1511959/cybercom-to-elevate-to-combatant-command/; Katie Lange, "Cybercom Becomes DoD's 10th Unified Combatant Command," DoD Live, May 3, 2018, http://www.dodlive.mil/2018/05/03/cybercom-to-become-dods-10th-unified-combatant-command/. [Cyber Command was established in 2009 as a subunified command of the U.S. Strategic Command.]

[103] Donald John Trump, *National Cyber Strategy of the United States of America [2018]* (Washington, DC: The White House, September 2018), 21.

[104] Mattis, *NDS 2018*.

[105] Mattis, *DCS 2018*, 1.

[106] Mattis, 3.

[107] Donald John Trump, "Executive Order 13848 on Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election," Presidential Actions, September 12, 2018, https://www.whitehouse.gov/presidential-actions/executive-order-imposing-certain-sanctions-event-foreign-interference-united-states-election/.

https://scholarcommons.usf.edu/mca/vol4/iss2/1
DOI: https://doi.org/10.5038/2378-0789.4.2.1076

[108] James R. Langevin, "Keynote Remarks by Congressmen James Langevin [D RI 02] Co-Chair of the Congressional Cybersecurity Caucus" (May 15, 2019), https://www.icsvillage.com/schedule-hack-the-capitol-2019.

[109] Sanger, "Pentagon Puts Cyberwarriors on the Offensive, Increasing the Risk of Conflict."

[110] Paul M. Nakasone GEN., "Statement of the Commander, United States Cyber Command / Director, National Security Agency / Chief, Central Security Service," § Committee on Armed Services (2019), 4, https://www.armed-services.senate.gov/hearings/19-02-14-united-states-special-operations-command-and-united-states-cyber-command.

[111] Paul M. Nakasone GEN., "A Cyber Force for Persistent Operations," *Joint Forces Quarterly*, no. 92 (January 2019): 11, http://ndupress.ndu.edu/Media/News/News-Article-View/Article/1736950/a-cyber-force-for-persistent-operations/.

[112] William T Eliason, "An Interview with Paul M. Nakasone," *Joint Forces Quarterly*, no. 92 (January 2019): 4.

[113] Nakasone, "A Cyber Force for Persistent Operations," 12.

[114] Nakasone, 12.

[115] C. Todd Lopez, "Cyber Command Expects Lessons From 2018 Midterms to Apply in 2020," U.S. Department of Defense News, February 14, 2019, https://dod.defense.gov/News/Article/Article/1758488/cyber-command-expects-lessons-from-2018-midterms-to-apply-in-2020/.

[116] Eliason, "An Interview with Paul M. Nakasone," 4–5.

[117] Mark Pomerleau, "What Good Are 'Exceptional' Cyber Capabilities without Authority?," Fifth Domain, July 17, 2019, https://www.fifthdomain.com/dod/2019/07/16/what-good-are-exceptional-cyber-capabilities-without-authority/.

[118] Sanger, "Pentagon Puts Cyberwarriors on the Offensive, Increasing the Risk of Conflict."

[119] Ellen Nakashima, "U.S. Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms," *The Washington Post*, February 26, 2019, Biography In Context.

[120] Nakashima.

[121] *USCYBERCOM Cyberspace Strategy Symposium Proceedings 2018* (National Defense University, College of Information and Cyberspace: U.S. Cyber Command, February 15, 2018), 7, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Cyberspace%20Strategy%20Symposium%20Proceedings%202018.pdf?ver=2018-07-11-092344-427.

[122] RM Staff, "Esper on Russia: Pentagon Nominee Sees Moscow as 'Strategic Competitor,' 'Potential Adversary.'"

https://scholarcommons.usf.edu/mca/vol4/iss2/1
DOI: https://doi.org/10.5038/2378-0789.4.2.1076