Strategic Blind-Spots on Cyber Threats, Vectors and Campaigns*

Dr. Cathy Downes

INTRODUCTION

In January 2017, the U.S. Office of the Director of National Intelligence published a highly unusual public report outlining the Russian state-sponsored cyber-enabled campaign to distract, disrupt, and skew the 2016 U.S. elections.[1] This latest influence campaign and continuing activities in both the U.S. and other Western countries are increasingly acknowledged as part of a broader, ambitious Russian strategy of strategic competition to restore its European sphere of influence, and erode other countries' subscription to the Western liberal economic and political order.[2]

There is a growing body of evidence[3] showing Russian strategists and agents aggressively employing and leveraging an eclectic mix of interventions, including cyber/physical world creation, sharing and exploiting of disinformation and private information through social media platforms, hacking, honeypots, harassment, social botnets, astroturfing, undermining of mainstream and social media sources and content, invasive espionage, theft and exposure applications and platforms. They have also created, cultivated and exploited "useful idiots", "fellow travelers" and "agent provocateurs" as well as cyber troops, trolls and trouble-makers to borrow from the Oxford Internet Institute's Computational Propaganda Research Project.[4] Also as Pomerantsev and Weiss observe: "Feeling itself relatively weak, the Kremlin has systematically learnt to use the principles of liberal democracies against them in what we call…"the weaponization of information, culture and money," vital parts of the Kremlin's concept of "non-linear" war."[5]

There is growing understanding of *what* has been done in the Russian campaign. Rather less consideration has been given to *why* the campaign has been able to achieve the effects evidenced. Certainly, some credit must go to the innovativeness of the

Dr. Cathy Downes has been a Professor of the National Defense University's College of Information and Cyberspace since 2003. She holds Ph.D. in International Relations and Strategic Studies from the University of Lancaster, United Kingdom. She is also an Australian Defense Industrial Mobilization Course graduate and holds a U.S. Department of Defense Chief Information Officer Certificate. Dr. Downes has held research fellowships at Harvard University's Center for International Affairs, University of Melbourne and Australian National University before serving as a senior civilian executive in the New Zealand Defense Force, leading enterprise transformation initiatives and as a defense policy writer and adviser. She leads the College's Cyber Leadership and JPME II program courses on National Security and Cyber Power Strategies and Multi-Agency Collaboration. Her research interests include: concepts of international cyber power, strategic thinking and national security strategy formulation, an inter-agency collaborative maturity model, technology futures assessments, and digitally-enabled learning environments.

Russians. Their "active measures" have evolved to leverage new capacities and target vulnerabilities created by the unique features and dynamics of cyberspace and Western populaces and their polities.

But it is also the case that the campaign's successes are partially due to miscalculation, and mistakes—strategic blind-spots—on the part of Western national security policy leaders and practitioners. These have created opportunities and weaknesses that Russian disinformation tactics have been able to capitalize on.

A "blind-spot" is an area of the eye's retina that is "insensitive to light." More colloquially, it is an inability to understand something or see how important it is. More pointedly, a blind-spot is a prejudice or area of ignorance that one has but is often unaware of. [6] Blind-spots cause or contribute to reasoning and decision failures—(1) not "connecting the dots" about causes and effects in time to take necessary action; (2) not imagining real possibilities and reacting accordingly, and (3) not taking corrective action. For national security policy leaders and professionals, strategic blind-spots create opportunities for being surprised by what they have not had the situational awareness to anticipate. Further, if a person or group is unaware of a blind-spot, and consequently does not address this defect, the likelihood of poor reasoning and decisions is substantively increased.

In the case of the Russian influence campaign leading up to and beyond the 2016 US elections, a number of strategic blind-spots can be highlighted. Recognizing and addressing these is critical to the design of effective deterrent and response national security strategies. Assumptions need to be challenged; cognitive biases recognized and corrected, and perspectives broadened. Sans these self-assessments, any strategic calculus to frame countermeasure strategies are likely to be insufficient or flawed, allowing conditions to persist that will aid future Russian and copy-cat cyber-enabled threats, vectors, and campaigns.

Overlooking a Critical Target and Underestimating Threats to it

The Y2K experience revealed the extent of dependence upon computer systems in highly industrialized societies and economies. Since then, this reliance has only increased and spread to every industry and government sector. The "surface area" to be secured continues to expand exponentially with developments such as IPv6, social media platforms, the Internet of Things, and global growth in Internet/mobile devices and users.

At the same time, the commercial first-to-market competitive pressures have often proven greater than warnings of the need for the early design of security features in products. As a consequence, the roll-outs of hardware and software have included bugs, flaws, and other vulnerabilities. These have been matched by the growth of an "alt" industry for building and distributing hacks and exploits that take advantage of or address these these vulnerabilities.

As a result, governments and businesses have fixated on defending and protecting their data, IT devices, systems, and networks from pernicious penetration and exploitation attempts and successes by state-sponsored and non-state cyber thieves, spies, hacktivists, and hoodlums. As one industry analyst observed: "IT analyst forecasts are unable to keep pace with the dramatic rise in cybercrime, the ransomware epidemic, the refocusing of malware from PCs and laptops to smartphones and mobile devices, the deployment of billions of under-protected Internet of Things (IoT) devices, the legions of hackers-for-hire, and the more sophisticated cyber-attacks launching at businesses, governments, educational institutions, and consumers globally." [7] The string of recent high profile cyber breaches and thefts have placed increasing pressures on governments and businesses to double-down on investing in cyber defenses. Dramatic estimates of the costs of these breaches, the costs of cybersecurity and workforce-related requirements reinforce the focus. [8]

In 2013, the Obama Administration issued Presidential Policy Directive 21—Critical Infrastructure Security and Resilience, which replaced the 2003 Homeland Security Presidential Directive 7 on the same subject. PPD-21 aimed at "...taking proactive steps to manage risk and strengthen the security and resilience of the Nation's critical infrastructure, considering all hazards that could have a debilitating impact on national security, economic stability, public health, and safety or any combination thereof. These efforts shall seek to reduce vulnerabilities, minimize consequences, identify and disrupt threats and hasten response and recovery efforts related to critical infrastructure." The Directive

* *The views expressed are those of the author. They do not necessarily reflect the policies of the U.S. Department of Defense, National Defense University or the College of Information and Cyberspace. The author wishes to thank Dr. Paul Shapiro and NDU CIC faculty for helping me clarify my thinking on a key aspect of this article.*

identified 16 “Critical Infrastructure Sectors” and matched each to a “Sector Specific Federal Agency or Department” under the overall coordination of the Department of Homeland Security.[9] The only sector of relevance to governing the nation was that of “Government facilities” being concerned primarily with protecting government buildings and national monuments and icons.[10]

Unfortunately, the concept of “infrastructure” was limited to physical structures, and technical control systems and assets. Inevitably, this approach channeled thinking and assessments of the types of threats that can, and are, threatening these targets, particularly regarding terrorism and cyber assaults. Within PPD-21 there are 16 critical infrastructures are drawn from those identified in the U.S.A. Patriot Act 2001 that defines criticality as being “so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety…” Most dictionary definitions of infrastructures also include the qualifier of being “needed for the operation of a society or enterprise.”[11]

When these perspectives are brought into a concept of critical infrastructure, it would seem that one infrastructure needed for the operation of a society was overlooked the US system of political governance; encapsulating a political system for choosing and replacing governments through free and fair elections whose results are accepted societally; active participation of citizens in politics and civic life; protection of human rights, and equality under the law.[12] Nested in this system are politicians, candidates for political office, political parties, campaigns, donors and staffs, constitutional provisions for elections, and most particularly the views, perspectives, beliefs, and understandings of eligible and future voters.

Yet, even when it became apparent by mid-2016 and through early 2017 that the Russians had engaged in a concerted information campaign against the 2016 elections, US government responses were dominated by technical thinking. This was demonstrated in the January 2017, decision to only modify the Government Facilities Critical Infrastructure Sector to include “the information, capabilities, physical assets, and technologies which enable the registration and validation of voters; the casting, transmission, tabulation, and reporting of votes; and the certification, auditing, and verification of elections.”[13]

The issue of foreign interference in the 2016 election had become a hot topic of discussion in 2017. Yet, within this, little concern seems to have been raised over the absurdity and inadequacy of taking actions to secure voting machines, *after* agents of a foreign power acted to subvert and manipulate the cognitive decision choices of voters before they even arrived at the polls. Lacking tools to show irrefutable evidence of impact, it would seem that it was merely assumed that foreign interference would have no impact on the minds and choices of voters. However, as further evidence of the extent and creativeness of the Russian influence campaign emerges, the grounds for this assumption are becoming more questionable.

Diverted by the obvious urgency to secure technical systems, national security policymakers and professionals failed to recognize the "weaponizing" of internet content as a threat, the US political system as an infrastructure of criticality for the effective functioning and security of the US government and society, and the voting public, as the target. In testimony before the U.S. Senate Armed Services Subcommittee on Cybersecurity, in April 2017 Rand Waltzman remarked: "Today...the manipulation of our perception of the world is taking place on previously unimaginable scales of time space and intentionality. That, precisely, is the source of one of the greatest vulnerabilities we as individuals and as a society must learn to deal with. Today, many actors are exploiting these vulnerabilities ...Information environment security today is primarily concerned with purely technical features...This view is too narrow." [14]

Strategy and Strategic Thinking Required as Much as Military Doctrine

The Royal United Services Institute (RUSI) Director of Military Sciences Peter Roberts observes that "...the West's understanding of war remains essentially Napoleonic: organized campaigns, orchestrated by a central staff...[but] the enemies of the West have reconstructed conflict and reimagined warfare to suit their own ends. Against this, the West has failed to appreciate...that way of considering the world, and remains bound by the codification of warfare put forward by Clausewitz, J.F.C. Fuller and Basil Liddell Hart...the Western focus is on the way adversaries act at the tactical level, not on understanding the nature of change that has occurred in their way of fighting. A belief in Western conceptual or intellectual superiority remains deeply entrenched in the Western orthodoxy; such hubris has distinct dangers." [15]

Evidence of Russia's influence and manipulation campaign supports Dr. Robert's tough and discomforting assessment that highlights a second blind-spot of US national security policymakers and practitioners. This concerns the dominant influence of military doctrine thinking and concepts upon US grand and national security strategy and strategic discourse.

Military doctrine serves to codify best military practices from primarily historical experiences. It is also used to translate...the higher conceptualization of war...into working guidelines for action." [16] There are risks in this power as British military historian Sir Michael Howard warns that: "...the soldier has to steer between the dangers of repeating the errors of the past because he is ignorant that they have been made, and of remaining bound by theories deduced from history although changes in conditions have rendered these theories obsolete." [17]

The evolution of US military and joint doctrine over recent years has had some relevant unintended consequences. For example, Kelly and Brennan in their 2009 U.S. Army War College Strategic Studies Institute monograph, *Alien: How Operational Art Devoured*

Strategy examine how the US doctrinal focus on the operational level of war, and operational art has in many ways supplanted strategic conceptualizations and consigned political and policy leaders to the role of "strategic sponsors." [18]

Over the last decade particularly, Russian civil and military leadership have evolved a broad and multi-faceted grand strategy for strategic competition with the Western liberal economic and political order. By contrast, US military doctrine, perspectives, mindsets, and priorities have become the significant dynamic in the meager space of Western and US strategic thinking and discourse devoted to the impact of cyberspace on international security relations, strategy and the strategic application of the information instrument of national power. Kelly and Brennan observe: "[operational art] has come to compete with strategy rather than being its humble servant." They question whether recent Western military failures are the result of endemic weaknesses or possibly due to: "...allowing operational art to escape from any reasonable delimitation and, by so doing, subvert the role of strategy and hide the need for a strategic art?" [19]

As discussed above, military understandings of cyberspace, cyber power, and strategy options that particularly leverage both, have been preoccupied with tactical and technical responses to threats to U.S. Department of Defense (DoD) computer networks and systems. As the strategic theorist, Colin S. Gray observes: "High-quality strategic theory about cyber simply is not there in the literature...The negative comparison with the nuclear debate in the 1950s is almost extraordinary in its scale and quality." He goes on to observe that: "...to risk understatement, most of this literature, though no doubt valuable in its own right, has been innocent of, or naïve about, strategic considerations." [20]

This is not to deny the significance of such threats or the vulnerability for US military forces whose technology development path over the last decades has focused on sustaining a conventional battlefield "speed of thought and adaption" edge through the advantages of enhanced situational awareness and self-organization enabled by networked information systems. In response, priority has been placed designing, resourcing and executing "cyberspace operations" to protect DoD and military missions in and through cyberspace. [21] The case for priority and attention has been intensified by high profile cyber thefts and evidence of mass attempts at network penetration.

Over the same period, comparatively, the significance and resources assigned to US military "information operations" [22] has faded. In the US, the case for such operations has been influenced by "...a peculiarly American outlook that using persuasion and influence at the national level is somehow unethical and inconsistent with a democracy, that using "psychological tricks" is "dirty" and immoral, and that it's completely unnecessary... the United States should just factually show the world who we are, and everyone will automatically recognize how wonderful we are and want to emulate us. The successful propaganda efforts of US enemies also contributed to the American distaste in many circles... Anything that smacked of propaganda or psychological warfare became something that only the "bad guys" did." [23]

Despite the energy of IO advocates, wide-scale and insightful understanding of changes in the information environment have been slow to gain traction in the US military doctrine and national security communities. The viral emergence of the interactive web, the blogosphere, the exponential growth and uses of social media platforms have tended to be restricted to a military context and sadly often limited to a narrow concern over whether troops and employees are being distracted from their work by "socializing on Facebook."

Doctrinally and legally, such operations have been treated only within the context of US military operations in overseas theatres and to support U.S. Combatant Commanders.[24] By contrast, the growing body of evidence of Russia's on-going "active measures" campaigns in Europe and the US shows that Russian civil and military leaders have elevated information operations to a full-blown instrument of strategic influence, both "narrative power"[25] and disruptive power, mainly taking advantage of national border-agnostic developments and capabilities of the interactive social Internet.

There has been an increasing divergence between Western and particularly US conceptions and approaches to strategic competition, conflict, war and military operations, and those of the national security communities of countries such as Russia and China. This is again well summed by RUSI Director of Military Science Roberts: "...the West's enemies see the battlespace as a whole, a global environment not confined by the limits the West has imposed on it...individual domains, areas, theatres and concepts are all linked and are intrinsically part of the contest. Boundaries do not exist for them, and where the West constructs them, they see weaknesses and vulnerabilities to exploit. They intrinsically use confusion, distraction, deception and obscuration to achieve long-term goals, accepting that failures and losses are part of that journey."[26]

Particularly post-September 11, 2001 attacks, with with a partial exception of the Obama Administration, US national security leaders have relied more intently upon the military instrument in national security strategy and statecraft. The US has doubled-down on its hard power capacities. In response, other lesser military powers have increased their leveraging particularly of the informational instrument's soft power advantages while continuing to upgrade their military capabilities organically and those for cyber espionage.

Moreover, in the most recent period, changes in US international policies have undermined many sources of national soft power.[27] This is somewhat ironic at a time when other national leaders have perceived the significance of leveraging soft power through, and in, cyberspace as one of the critical changes in nature of international strategic competition, and acted upon that perception, as Director of the European Council on Foreign Relations, Mark Leonard remarks: "The most important battleground of this conflict will not be the air or ground but rather the interconnected infrastructure of the global economy: disrupting and controlling trade, investments, currencies, international law, the internet, transport links, and the movement of people, employing boycotts, sanctions, disinformation, Welcome to the connectivity wars."[28]

Following his analysis of the Arab Spring, it is interesting to note the Russian Chief of the General Staff's 2013 reflections on how the Western way of war had evolved, perceptively observing a four-to-one ratio of non-military to military measures. General Gerasimov and others in the Russian national security community have possibly read more strategic calculus and coordination in Western actions than is merited. Nonetheless, it would seem that Russian leaders have followed this ratio in designing a grand strategy of competition that leads with the information instrument of national power's 21st century disinformation and cognitive hacking interventions.

Historically, Western military doctrine has regularized novel conditions and capabilities by fitting them into accepted ways of organizing and thinking. In each case, an internecine dynamic plays out where some advocates seek to create new distinct structures, authorities, and practices while others seek to fit new conditions and capabilities into extant unit, rank structures, tactics, techniques and procedures, and culture. The press to institutionalize cyberspace (as the fifth domain) and cyber capabilities within extant US military models is evident in actions such as the standing up U.S. Cyber Command (USCYBERCOM), its 2017 elevation as a full unified combatant command, the 2015 DoD Cyber Strategy [29] and multi-million dollar resourcing of "Cyber Mission Forces" cyber "warrior career" paths, etc. with the primary emphasis on forces and capabilities for protecting and defending DoD networks and systems, and supporting the needs of U.S. Joint Force Commanders in the conduct of conventional operations.

The focus of these efforts is underpinned by an untested assumption: that the other US military services, joint organizations and operational doctrine offer the best model for organizing information and cyberspace national security capabilities. Yet, if we take as a small point of comparison: while the US has focused its investment on developing regularized military professional Cyber Mission Forces, the Russian Federation has invested in, sponsored and leveraged an eclectic lineup of irregular, civilian hackers, ad click-bait entrepreneurs, proxy non-governmental organizations, automated computer algorithm botnets, "useful idiots" within the US and other Western countries, and a low-cost, deniable, easily-expandable "troll army" of social media commentators and post authors. [30]

This comparison is not to recommend that the US match Russian troll armies. It is to suggest that a purely military model of capabilities and structures for responding to information and manipulation campaigns may not necessarily be optimal.

Legitimizing novel conditions and capabilities by incorporating them into proven and prescriptive operational military doctrine models is also pre-empting intellectual efforts to assess and explore the impact of cyberspace upon international security relations. As a consequence, we have seen the comparatively uncritical transference of concepts of international security relations that have evolved within and respond to a quite particular and different strategic context. A classic example of this is the US defense community-sponsored push to formulate concepts of cyber deterrence. As MIT's Nazli Choucri's points out: "When we compare these unique and defining characteristics of cyberspace, it is evident that the major trajectories, dynamics and consistencies of international relations, established particularly throughout most of the 20th century cannot be readily or uncritically imported into international relations in and through cyberspace in the 21st century." [31]

This raises the more significant question as to whether the conditions and dynamics of cyberspace require an *a priori* period of similar critical examination to that given by international relations scholars, thinkers, and strategists during the 1950s and 1960s about strategizing to cope with the advent and proliferation of nuclear weapons. One of those scholars, Professor Brodie, in *Strategy in the Missile Age* (1959) observed: "There is an intellectual no-man's land where military and political problems meet. We have no tradition of systematic study in this area, and thus few intensively prepared experts. The military profession has traditionally depreciated the importance of strategy (where politics are important) as compared with tactics. Now we are faced with novel and baffling problems to which we try to adapt certain ready-made strategy ideas inherited from the past." [32]

While the destructive capacity of nuclear weapons is proven unequivocally and the possible destructive effects in cyberspace are not, arguably we are in a similar intellectual no-man's land. Cyberspace, and its demonstrated and evolving potential uses for strategic effect, do not fit neatly into existing operational and strategic concepts. Instead of borrowing and shoe-horning existing strategic and international relations concepts, there is a need to devote strategic thought into formulating more original strategy and foreign policy ideas and approaches that can appropriately guide military doctrine thinking and development.

Finally, in many respects, it would seem that the US national security establishment has fallen foul of the national security blind-spot equivalent of Harvard University's Professor Clayton Christensen's Innovator's Dilemma. [33] As noted above, unable to compete directly with the U.S. military power advantage, countries, such as Russia and China, have evolved strategies favoring less expensive, more adaptive non-military instruments of national power, while continuing to build up their military capabilities. As with Christensen's model for businesses, the US has focused on ever expanding the over-match of its military power capabilities to counter the military capabilities of competitors. [34]

In Christensen's business model, new entrants with few resources innovate with technologies and markets, producing goods and services viewed by mainstream businesses as cheap, tacky, and lacking in features attractive to their customers. As a consequence, new entrants are not viewed as threats. Failure comes when the upstart advances rapidly entering the more mature markets of incumbents and disrupting them. [35] While certainly not new entrants, re-emergent and revanchist powers, such as China and Russia, are playing the new entrant role.

Thus, while the US defense community and industrial base has been preoccupied with over-matching the military capabilities of competitors, the Russians have applied an out-flanking strategy-level "offset" of a different sort. As Paul and Matthews: "Russia has taken advantage of technology and available media in ways that would have been inconceivable during the Cold War...Experimental research in psychology suggests that the features of the contemporary Russian propaganda model have the potential to be highly effective." [36]

In concentrating on cyber threat vectors for obvious data and information theft, malware, denial of service assaults to the technical layers of cyber infrastructure, and on over-matching conventional and strategic military capabilities, national security policy makers and practitioners have overlooked the larger cyber-based threats to the US political system that have been created. Klimberg observes: "through a subtle reframing of information overall as a weapon...we have moved toward a reconceptualization of interstate conflict and "war" altogether, one where states routinely engage in hostile acts that skirt around and under the threshold of recognized war and increasingly manage to reposition "information" including everything from computer viruses to the workings of the media, as a weapon, with potentially existential implications for democratic societies." [37]

Strategic Center of Gravity or Critical Vulnerability or Both?

All US National Security Strategies declare: "The United States government has no greater responsibility than protecting the American people." [38] Yet, both national and subordinate strategy documents, such as the national military strategy, narrowly focus only on conventional threats of kinetic violence employing land, maritime and/or air-deployed weapons and tactics, or the unconventional threats of violent extremist groups.

This assessment leaves unconsidered threats that do not depend on destruction of life and property to achieve desired outcomes, including "...the use of information and communication technologies, services, and tools to create and spread stories intended to subvert and undermine an adversary's institutions, identity, and civilization, and it operates by sowing and exacerbating complexity, confusion, and political and social schisms." [39]

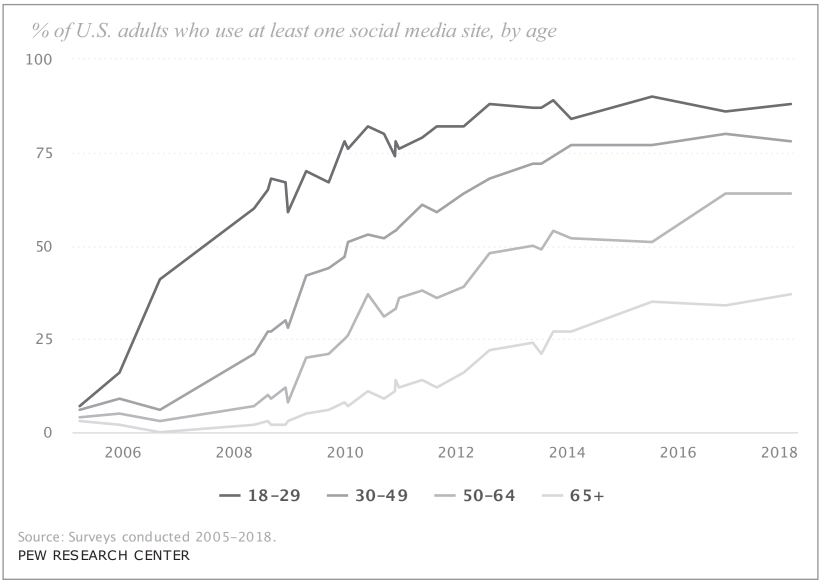
Any robust threat assessment focuses on two factors—the threat's intentions and capability, and the strengths and defenses of that which is threatened. Yet, the US national security community has underestimated the threat posed by Russia's grand strategy and influence campaign. It has also underrated, if not assiduously avoided assessing, the vulnerabilities of the US populace and polity, and Western partners and allies, to being targeted by this campaign. Overlooking these vulnerabilities substantially weakens any strategic calculus for effectively countering such tactics.

An examination of conditions and circumstances shows the US population and its political system as a particularly soft target, as Brad Allenby observes: "...a number of trends are coming together to create a unique historical period, one in which weaponized narrative not only has a privileged position as a weapon of choice to use against otherwise conventionally well-armed adversaries, but in which the United States is uniquely vulnerable." [40]

Dependent upon free-and-fair citizen elections to legitimize changes of government, representative democracies provide scheduled and frequent targets for disinformation campaigns. This dependence and the opportunity it provides is not new. What has changed is the vulnerability of voters to manipulation that leverages their increasingly rich and predictive digital foot-prints. Data and information about voters preferences and predispositions is increasingly for collection and sale through new enabling applications for online and offline shopping, internet search data on habits, financial transactions, online news viewing, commenting and sharing, cell phone usage, blogging, virtual worlds, social and video communications via online media platforms, the Internet of Things and data from surveillance devices. While primarily generated for commercial marketing purposes, the populace's Internet engagement has provided an exponentially expanding equal-opportunity source of data for political campaigns *and* foreign disinformation campaigns.

Such databases can significantly empower political campaigns and candidates to engage and inform potential voters cost-efficiently. At the same time, the data trails left by voters provides campaigns with the increasing ability to psychometrically profile, compose and target messages to individual voters that intensify and amplify, rather than reduce, their cognitive biases and preconceptions; that can disinform as much as inform. Evidence continues to build of such leveraging of voter data in the US 2016 election being used to manipulate voter choices about their intentions about voting and how to vote raising the possibility of indirect suppression and invalidation of votes. Notable example of these tactics included the data and predictive analytics and ad micro-targeting employed by UK Company, Cambridge Analytica, and the use of targeted deceitful and misleading content messages through the Facebook and Twitter platforms such as the fraudulent vote-by-text message. [41]

The US population is particularly vulnerable to such targeting because of its high reliance on cyber interconnectivity, sourcing of news and social/political engagement. For example, in 2016, the global average internet penetration was 50%; for the United States, it was 88%. For social media penetration, the global average was 37%; for the U.S. it was 66%. In comparison to the 55% global average, 70% of US Facebook users use the platform daily. [42] In Pew Research Center surveys, in 2005, just 7% of American adults used social networking sites. By 2017, 69% of American adults used such sites and of those Americans using Facebook, just under half (45%) get their news from Facebook, and 26% of all US adults get news from two or more social media sites. [43]



% of U.S. adults who use at least one social media site, by age

Source: Surveys conducted 2005-2018.
PEW RESEARCH CENTER

http://www.pewinternet.org/fact-sheet/social-media/

Appearing before the U.S. Senate Select Committee on Intelligence in late 2017, Facebook's Legal Counsel, Mr. Stretch testified that Facebook had identified "... a total of 80,000 posts and ads from Russian-backed accounts [from one source—the Russian Internet Research Agency] were seen by 126 million people through flow-on effects of interconnected users, uncritically sharing with other users in their personal networks over a period of two years." Twitter and Google Legal Counsels also presented estimates of Russian activities on Twitter and YouTube.[44] These numbers were down-played disingenuously referencing the larger scale of total activity on these platforms. However, it would seem that Russian-backed disinformation posts and ads reached over 50% of Facebook's US users. Moreover, no assurance was given that the full scope of Russian disinformation activities had been discovered.[45] Further, these figures do not reflect the additional effects of data analytic companies leveraging data on users' sharing and "likes" to tailor ad buys to disseminate intentionally or unintentionally similar sentiments and messages to those of Russian engineered content.

The degree of connectivity is also reflected in the broader Facebook "universe" of ways in which people (and computer-algorithm social bots acting as people) can share disinformation and their own personally identifiable data as much as information. These include Facebook-owned social media messenger and chat apps—Facebook Messenger, WhatsApp and Instagram with duplication through easy-use cross-posting between these apps. These all increase the scale and density of virtual tributaries and arteries that can be penetrated and leveraged by disinformation campaigns not only by Russia but also by a variety of existing and future non-state actors.

Significant upgrades in mobile devices, interactive web and blog apps, livestreaming capacities, and monetarization models have all reduced entry barriers—or "democratized" —the human and botnet creation and wide-scale distribution of all types of "news" content, including an increasing array of user-produced video.[46] This has substantially expanded the scope and availability of unfiltered, un-aggregated, and un-mediated content that Americans are exposed to through their Facebook accounts and in the broader Internet. This content access is also influenced by online news aggregator and filter bubble apps that tailor and shape what users view, read or interact with.[47]

Further, earlier Soviet-era influence campaigns had the goal of weaving a strategic narrative of a positive image of the communist political and economic system. By contrast, the contemporary Russian campaign in the US 2016 elections, for example, appear to have shifted to a more achievable and less challenging goal; that of promoting distraction, confusion, doubt and mistrust, with almost an equal-opportunity approach to targeting disinformation, emotionally charged histrionic news items and comments on all sides of the political spectrum. For example, in looking at Russian "information warfare," Keir Giles observes: "...Unlike in Soviet times, disinformation from Moscow...has as one aim undermining the notion of objective truth and reporting being possible at all...the new vulnerability that current Russian campaigning can exploit is, in the words of veteran scholar of Russia Leon Aron, Western societies' "weakened moral immunity to propaganda" and "weakness of confidence in sources of knowledge."[48]

As a consequence of the density and diversity of connectivity and the proliferation of content, voters are increasingly overwhelmed and under-equipped to distinguish fact from fiction. Distinguishing whether any, all or some content is truthful, useful, or customized disinformation inserted by foreign state agents or non-state actors or legitimate political campaigns is increasingly challenging. Moreover, as online advertising have successfully drawn off ad revenues from "mainstream" media organizations, such organizations, even in their online formats, have had fewer resources to serve as filters for objectivity and accuracy.[49] Furthermore, responses to information overload also can have particular counter-intuitive effects that are not necessarily recognized by voters. For example, Paul and Matthews in examining the Russian propaganda model note that: "When information volume is low, recipients tend to favor experts, but when information volume is high recipients tend to favor information from other users...The experimental psychology literature suggest that all other things being equal, messages received in greater volume and from more sources will be more persuasive. Quantity does indeed have a quality all of its own."[50]

Exposed to overwhelming amounts of information, steered by filters and news aggregators, and targeted by their cognitive biases and digital footprints, it is not surprising that a portion of the electorate has been deceived by content that caused confusion, distraction, distrust or a retreat into an echo chamber that reinforced their preferences. This too has served both the goals of legitimate political campaigns and foreign influence campaigns, as once deceived, it is extremely difficult for anyone to admit that they have been gulled, and the evidence threshold for such an admission is commensurately heightened.[51]

The health of political discourse itself makes the US population and polity particularly vulnerable to cyber-enabled disinformation campaigns. Such campaigns delight in high levels of political discord and discontent. There are always going to be differences of opinion on any issue. However, partisan US political discourse has become deeply polarized in the last decades. The Pew Research Center's October 2017 survey observed that: "The divisions between Republicans and Democrats on fundamental political values—on government, race, immigration, national security, environmental protection and other areas–...have increased dramatically...And the magnitude of these differences dwarfs other divisions in society, along such lines as gender, race and ethnicity, religious observance or education."[52] The greater the degree of difference of political viewpoints and values, the greater the number and intractability of "wedge" issues, the more openings for disinformation messaging by foreign agents, indistinguishable from those of domestic political campaigns, which intensify and amplify distrust and disagreement with "the other."

At the same time, in the intensifying competition between television and online media organizations to sustain commercial viability by "...harvesting human attention and reselling it to advertisers," political discourse has become sensationalist political theatre, to entertain, not necessarily inform. Elections are political dramas. Contextualized as slap-down grudge matches, events are analyzed minutely and re-hashed by 'expert commentators' representing particular polarized viewpoints and opinions. The almost oxymoronic continuous "Breaking News," "Countdown" clocks to candidate debates which are themselves aired and streamed online as gladiatorial gotcha contests, are designed to grab and hold viewer attention. This is in addition to the efforts of political campaigns to out-do each other in both the frequency and shock/scandalize factor spin-doctored half-truth negative attack advertising on television, in robo-telephoning and distributed through web-and social media-based micro-targeted messaging.

Add into this cacophony of attention seeking sound-bites, where nothing can be denied for fear of a First Amendment Right to Free Speech challenge, the internet-leveraging "click-bait" entrepreneur.[54] Such actors purposefully eschew accurate, objective professional standards of journalism, recognizing that strongly negative or positive headlines tend to attract more viewers and therefore earn them more ad dollars.[55] Moreover, it is difficult for viewers to distinguish the motivations and origins of such actors—purely financial, foreign or domestic, political advocacy, or part of a Russian or non-state actor disinformation and manipulation campaign.

The quality of political discourse in the US 2016 election was further influenced by a significant increase in the exposure of voters to “fake news” or “distorted signals uncorrelated with the truth” mainly conveyed through social media platforms and websites designed to influence or confuse voters contextual understanding and candidate/party choice. Allcott and Gentzkow in their research findings on a database of just 156 false election-related news stories on social media assess that there was upwards of 760 million instances of a user clicking through and reading one of these 156 fake news stories. They note that a list of fake news websites, on which just over half of articles appear to be false, received 159 million visits during the last month of the election.[56]

Unfortunately, voters have not been helped to identify and distinguish accurate, objective, factual information from falsehoods and fabrications by the recent political practice of diversionary labeling of inconvenient or uncomfortable information as “fake.” Moreover, this practice has opened up a small industry in fact-checking sites that in turn have generated Russian government and likely government-sponsored fake fact-checking sites that label accurate information as fake.[57]

At the same time, there has been an increase over the last decade particularly in policy advocacy groups paying universities and think-tanks to secure academic credibility for their particular agendas[58] This has likely reduced the uniquely valuable contribution such institutions make to the plurality of in-depth research and analysis of critical policy issues. This robust diversity is an essential part of broadening and testing ideas and proposals in political discourse and policy debates. It is also crucial for exposing, for policymakers and practitioners, policy positions based on falsehoods, and biased analysis.[59]

Opening the Aperture

The physiological blind-spot in the human eye is where the optic nerve takes up the space of retina cells. The brain has an autonomic response that “fills in” information about what is most likely in the missing area. By contrast, the strategic blind-spots outlined above do not have a similar aid. Where they have been spied, most US national security policymakers and practitioners recognize them as wicked problems with innumerable causes; lacking a right answer; the opposite of hard but ordinary problems, which can be solved in a finite time by applying standard techniques; and where conventional processes fail, they may exacerbate situations generating undesirable and unintended consequences.[60]

Furthermore, the US national security policymaking architecture that should address these blind-spots is fragmented and fractious. It is bifurcated and bounded into externally and domestically facing sets of constitutional, administrative and legal precepts and arrangements. Like other contemporary issues (climate change, globalization, cyberspace governance), these arrangements, designed for the US political context of the late 1700s, are ill-equipped to respond to threats such as the Russian influence campaign. State

Department Public Diplomacy is legally bound to gaining foreign publics' support for US national interests.[61] The Department of Homeland Security limits its protection to how it defines Critical Infrastructure that only calls for protecting hardware and software, not human wetware. The DoD defends its computer networks. The Department of Health and Human Services and Centers for Disease Control and Protection each have their bounded area of specialist expertise and responsibility etc. for the American people. As Klimberg observes regarding cybersecurity but which applies equally well to efforts to respond to the Russian information campaign: "...each distinct aspect of cybersecurity... operates ...a specific government department or ministry. Each of these silos has its own technical realities, policy solutions and even basic philosophies...it is likely that you will not have the time to acquire more than a rudimentary knowledge of the others. Your part of the elephant will dominate and inevitably distort how you see this beast."[62] These structural divides are also mirrored in the division of law, authority and resourcing priorities at the state and local levels that challenge issues requiring national coordination and collaboration.

Thus, US governance systems struggle for systemic, whole-of-government approaches. This leaves a confusion of duplication and overlap as well as the vulnerability of seams and gaps so that little is provided to assist voters, political campaigns, and government leaders to distinguish between legitimate, First Amendment protected information and injects of disinformation by foreign agents or non-state actors. Moreover, these systemic challenges impede efforts to design and execute effective national security and cyber power strategies to address Russia's grand strategy of strategic competition with the West and the US in particular, and its use of cyberspace and information interventions to shape the security environment short of kinetic war.

Furthermore, given that effective strategy formulation requires context, there is a critical need to examine the next likely steps that the Russians may take. On the one hand, there is a natural inclination to "stick with a winning formula." Many US national security analysts and researchers are exposing the effects of the Russian information campaign during and after the 2016 US elections. Why quit doing what you are doing when it is evident that you are doing well?

On the other hand, unlike the physical air, land, sea and space domains, cyberspace and its data and information are constantly morphing and expanding as new technologies, opportunities, and risks for their use are created, as co-founder and chairman of the X-Prize Foundation Peter Diamandis remarked in February 2017: "advances in quantum computing and the rapid evolution of AI and AI Agents embedded in systems and devices in the Internet of Things will lead to hyper-stalking, influencing and shaping of voters and hyper-personalized ads, and will create new ways to misrepresent reality and perpetuate falsehoods."[63]

For example, expect new applications to manipulate video, transferring the idea of creating fake images and false text, tweets and retweets, to composing fake virtual reality/holographic projections for use in video. Political campaigns will need to prove that videos/TV presentations/commentators/leaders are real not fake. We are also likely to see advances in persuasive technologies to influence users through queuing autonomic responses to superficially innocuous messages for action.[64] Inevitably, developments in machine learning will make it almost impossible to distinguish a bot from human and human from a bot. We may need to rethink Abraham Lincoln's maxim that: "You can fool all the people some of the time and some of the people all the time, but, you cannot fool all the people all the time" as Helbing et al. remarks: "We are being remotely controlled ever more successfully...The trend goes from programming computers to programming people...a sort of digital scepter that allows one to govern the masses efficiently without having to involve citizens in democratic processes."[65]

The Russians may take a low-risk approach of doubling-down on their extant playbook of disinformation tactics and tools to replicate, if not entrench, the conditions of distraction, confusion, and distrust they have generated to date. The risk in this is that the US and Western allies will develop information intervention strategies to counter such efforts. Alternatively, they could change out the playbook with new combinations of existing and emerging data and information manipulation tools and tactics.

This prospect doubles the challenges for US and Western national security policy leaders and practitioners. There is a need to recognize and address strategic blind-spots impeding and diverting accurate threat and target identification that informs the development of effective strategies. Then, there is the need to formulate and execute strategies that can blunt and overturn current Russian information manipulation efforts *as well as* keep a countering pace in designing complementary diplomatic, informational, military and economic interventions that outflank how the Russians may choose to evolve their playbook.

Such strategies are beyond the remit of this paper. However, there are some actions that may contribute to improving the necessary conditions for sound strategy work by addressing the strategic blind-spots outlined here. Admittedly none are uncontentious or easy quick wins or low-hanging fruit. This is unrealistic when dealing with a wicked problem. The first and obvious recommendation is that policy leaders and practitioners recognize the US political system as a critical infrastructure, essential for the peaceful, stable functioning of a democratic American society, which is being threatened and targeted and requires national protection.

Policy leadership is needed to prioritize and resource at least five major research and development initiatives. The first concerns engaging with the broader national and international security relations and advanced technologies academic community in a concerted research initiative on the international security relations of cyberspace and cyber power.

The aim of this initiative would be to adapt existing concepts of international security relations and formulate original concepts of cyber power to better guide diplomatic and military interventions.

The second concerns a concerted research effort on emerging bio-robotic-info-nano technologies that could create new tactics and tools for both disinformation and for transparency. There is a need to examine the opportunities for foreign state actors, but equally copy-cat or original campaigns by non-state actors. Such an initiative should engage policy advisers, practitioners, industrialists, academics, and non-traditional participants. In a similar way to leveraging Hollywood screenwriters and directors who were reportedly asked by the U.S. Army to think up terrorist scenarios after the September 11 attacks, this research effort should engage diverse contributors from psychology, history, sociology, international security relations, political and behavioral sciences, advertising, marketing and strategy backgrounds.

The third concerted research effort needs to be led by the tech industry to design applications, protocols, machine learning features, rating systems, that *a priori* alert users to false/misleading information and disinformation before they interact with it. After-the-fact, fact-checkers are a whack-a-mole non-solution. Similar in concept to Secure Socket Layer Certificates for example and other applications that identify high-risk sites, and allow users to configure their settings to filter them out, the aim would be to tag disinformation sites and their content with the cyber equivalent of radioactive tracers or labels.

The fourth concerted research effort needs a "top-minds" legal taskforce to examine the weaknesses and vulnerabilities of US laws regarding regulations on political campaign advertising, "hate speech," privacy and control over personal data and information, etc. While any regulatory effort is likely to conflict with the First Amendment, this does not detract from the necessity of such a review and what it may find.

Finally, there is a need for an educational research and development effort to create easy-to-deploy-and-access learning opportunities that help K-12 and tertiary level students, the workforce, seniors, strategic policy leaders, government professionals develop critical digital literacies which are defined as: "the ability to use information and communication technologies to find, evaluate, create, and communicate information, requiring both cognitive and technical skills." [66] Such literacies are not new. However, too often, they have been reduced to matters of computer "hygiene habits" updating virus protections and Google searches. New learning experiences are needed for wide-scale implementation that focus on helping voters and users in cyberspace significantly heighten their acuities and skills to evaluate the quality, rigor of information and how their cognitive biases can be taken advantage of. As Allcott and Gentzkow observe and quote: "...the social return to education includes cognitive abilities that better equip citizens to make informed voting decisions. For example, Adam Smith (1776)," The more [people] are instructed, the less liable they are to the delusions of enthusiasm and superstition, which, among ignorant nations, frequently occasion the most dreadful disorders.”[67]

NOTES

1. Office of the Director of National Intelligence, (2017, January 06), ***Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*** (Washington D.C.).

2. As Rogers and Tyushka summarize the goals being pursued by Russia's "strategic narrative offensive" as seeking to: *1) 'desynchronise' political developments in the European Neighborhood to 'distort' European perceptions of reality; 2) 'de-articulate' the West, i.e., splitting the Atlantic democracies from the European mainland; and 3) 'saturate' the vacuum with false and fictitious narratives, to sow confusion and maintain manageable disorder.* James Rogers and Andriy Tyushka, (2017, March) "'Hacking' into the West: Russia's 'Anti-hegemonic' Drive and the Strategic Narrative Offensive" *Defence Strategic Communications* Vol. 2, 35, https://www.stratcomcoe.org/james-rogers-andriy-tyushka-hacking-west-russias-anti-hegemonic-drive-and-strategic-narrative, accessed on May 12, 2017.

3. The Russian influence campaign activities and tactics are well explored in a number of research reports and testimonies; for example, Braden R. Allenby, (2017, Summer), "The Age of Weaponized Narrative or, Where Have you Gone, Walter Cronkite?" *Issues in Science and Technology* (2 and 4), 65-70; Chengcheng Shao, e.al. (2017, July 24), "The Spread of Fake News by Social Bots" (https://arxiv.org/abs/1707.07592) (Accessed on July 25, 2017); Clint Watts (March 30, 2017), "Clint Watts' Testimony: Russia's Info War on the U.S. Started in 2014. The Daily Beast, http://www.thedailybeast.com/clint-watts-testimony-russias-info-war-on-the-us-started-in-2014, accessed on July 18, 2017; Watts, Clint, (2017, April 27) "Inside Russia's Fake News Playbook" The Daily Beast, http://www.fpri.org/article/2017/05/inside-russias-fake-news-playbook/, accessed on July 18, 2017; ibid., Howard Bradshaw, 2017; Edward Lucas and Peter Pomeranzev, (2016, August) *Winning the Information War – Techniques and Counter-Strategies to Russian Propaganda in Central and Eastern Europe* (Washington D.C., Center for European Policy Analysis), https://cepa.ecms.pl/files/?id_plik=2773, accessed on May 9, 2017; Heather A. Conley, et.al., (2016, October) ***The Kremlin Playbook – Understanding Russian Influence in Central and Eastern Europe*** (Washington D.C. Center for Strategic and International Studies, https://www.csis.org/analysis/kremlin-playbook, accessed on May 10, 2017); Shawn Powers and Markos Kounalakis, (Eds.) (2017, May) ***Can Public Diplomacy Survive the Internet? Bots, Echo Chambers and Disinformation*** (Washington D.C. U.S. Department of State, Advisory Commission on Public Diplomacy), https://www.state.gov/documents/organization/271028.pdf, accessed on May 10, 2017; Martin Kragh and Sebastian Asberg, (2017) "Russia's Strategy for Influence through Public Diplomacy and Active Measures: the Swedish Case" ***Journal of Strategic Studies;*** Published online January 5, 2017; Schreier, (2012) ***On Cyberwarfare*** (Geneva Centre for the Democratic Control of Armed Forces), http://www.dcaf.ch/Publications/On-Cyberwarfare, accessed on June 12, 2017; Brad Allenby and Joel Garreau (2017) ***Weaponized Narrative: The New Battlespace*** (Arizona State University, Center on the Future of War), https://weaponizednarrative.asu.edu/publications/weaponized-narrative-new-battlespace, accessed on July 24, 2017; Alice Marwick and Rebecca Lewis (2017, May) ***Media Manipulation and Disinformation Online*** (New York, Data and Society Institute), https://datasociety.net/output/media-manipulation-and-disinfo-online/, accessed on July 10, 2017; Emerson T. Brooking and P.W. Singer (2016, November) "War Goes Viral–How Social Media is Being Weaponized" ***The Atlantic*** 318, 4, 70-83; Ferrara, Emilio, et.al., (2015), "The Rise of Social Bots" Communications of the ACM 59, 7, 96-104, https://cacm.acm.org/magazines/2016/7/204021-the-rise-of-social-bots/fulltext, accessed on June 12, 2017; Alessandro Bessi and Emilio Ferrara (2016, November) "Social Bots Distort the 2016 U.S. Presidential Election Online Discussion" ***First Monday*** 21, 11, http://firstmonday.org/ojs/index.php/fm/article/view/7090/5653, accessed on July 15, 2017; Janus Bugajski, (2017), "The Geopolitics of Disinformation" (Centre for European Policy Analysis), http://www.infowar.cepa.org/The-geopolitics-of-disinformation, accessed on June 20, 2017; Sergey Sanovich, (2017), ***Computational Propaganda in Russia: The Origins of Digital Misinformation*** (Oxford, Oxford University Internet Institute, Working Paper No. 2017.3), http://comprop.oii.ox.ac.uk/2017/06/19/computational-propaganda-in-russia-the-origins-of-digital-misinformation/, accessed on July 17, 2017; Matthew Ingram (2017, May 31), "Trump's Fake Twitter Following Climbs, Sparking Fears of a Bot War" ***Fortune Magazine,*** http://fortune.com/2017/05/31/trump-twitter-bot-war/, accessed on July 17, 2017; Dhiraj Murthy, et.al. (2016) "Bots and Political Influence: A Sociotechnical Investigation of Social Network Capital" ***International Journal of Communication*** 10, 4952–4971; Christopher Paul and Miriam Matthews () The Russian "Firehose of Falsehood" Propaganda Model Why It Might Work and Options to Counter It" ***Rand Perspectives,*** http://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf; Rand Waltzman, (2015, September) The Weaponization of the Information Environment" ***American Foreign Policy Council Defense Technology Program Brief*** No. 12, 4-9.

4. Phillip Howard (2017, July 14), ***Troops, Trolls and Trouble-Makers: A Global Inventory of Organized Social Media manipulation*** (Oxford, Oxford Internet Institute), https://www.oii.ox.ac.uk/blog/troops-trolls-and-troublemakers-a-global-inventory-of-organized-social-media-manipulation/, accessed on August 14, 2017.

5. Peter Pomerantsev and Michael Weiss, (2014) The Menace of Unreality: How the Kremlin Weaponizes Information, culture and Money (Washington D.C. Institute of Modern Russia, http://www.interpretermag.com/wp-content/uploads/2015/07/PW-31.pdf, 4.

6. https//www.collinsdictionary.com/us/dictionary/English/blind-spot, accessed on October 29, 2017.

7. Steven Morgan, (2016, June 15), "Cybersecurity spending outlook: $1 trillion from 2017 to 2021" ***CSO Online,*** https://www.csoonline.com/article/3083798/security/cybersecurity-spending-outlook-1-trillion-from-2017-to-2021.html, accessed on November 12, 2017.

8. See for example, Accenture, (2017) ***2017 Cost of Cyber Crime Study,*** https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf, accessed on November 28, 2017.

9. The White House, (2013, February 12), Presidential Policy Directive 21– Critical Infrastructure Security and Resilience, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil, accessed on October 9, 2017.

10. U.S. Department of Homeland Security, General Services Agency, (2015), ***Government Facilities Sector-Specific Plan,*** Annex to National Infrastructure Protection Plan 2013), 1, https://www.dhs.gov/sites/default/files/publications/nipp-ssp-government-facilities-2015-508.pdf, accessed on October 12, 2017.

11. https://en.oxforddictionaries.com/definition/infrastructure, accessed on November 28, 2017.

12. Larry Diamond, (2004), "What is Democracy?" (Lecture at Hilla University for Humanistic Studies), http://web.stanford.edu/~ldiamond/iraq/WhaIsDemocracy012004.htm, accessed on November 28, 2017.

13. Secretary of Homeland Security Mr. John Kelly, (2017, June 13), Letter to The Honorable Claire McCaskill, Committee on Homeland Security and Government Affairs, U.S. Senate. Kelly goes on to note: *"DHS, in coordination with partners from the Intelligence Community, federal law enforcement, and MS-ISAC, observed Russian cyber actors attempting to access voter registration databases prior to the 2016 elections . . . Based on the observed threat, DHS focused its efforts on providing election officials with information to protect their internet-connected election infrastructure, such as voter registration databases, election websites that provided information for voters on where to find their polling places, and election night reporting systems."* Here again, the focus was on access to voter registration data bases, not access to voter's beliefs, information, etc.

14. Armed Services Committee, Subcommittee on Cybersecurity, (2017, April 27), ***The Weaponization of Information – the Need for Cognitive Security*** (Testimony: Rand Waltzman), CT-473, Senate.

15. Peter Roberts, (2017, February/March) "Designing Conceptual Failure in Warfare – The Misguided Path of the West" ***RUSI Journal,*** 162, 1, 17-19.

16. John Gooch, (ed.), (1997, September) ***The Origins of Contemporary Doctrine*** (Camberley, Surrey, Strategic and Combat Studies Institute, Occasional Paper no. 30), 5.

17. Quoted in Charles Grant (1997), "The Use of History in the Development of Contemporary Doctrine" in John Gooch (ed.), (1997, September), The Origins of Contemporary Doctrine (Camberley, Surrey, Strategic and Combat Studies Institute, Occasional Paper no. 30), 10.

18. Justin Kelly and Mike Brennan, (2009, September), ***Alien: How Operational Art Devoured Strategy*** (Carlisle Barracks, PA, U.S. Army War College, Strategic Studies Institute Publication 939), https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=939, accessed on December 1, 2017.

19. Justin Kelly and Mike Brennan, (2009, September), Alien: How Operational Art Devoured Strategy (Carlisle Barracks, PA, U.S. Army War College, Strategic Studies Institute Publication 939), https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=939, accessed on December 1, 2017, 4.

20. Colin S. Gray, (2013, April), Making Strategic Sense of Cyber Power; Why The Sky is Not Falling" (Carlisle PA., U.S. Army War College, Strategic Studies Institute Publication No. 1147, https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1147, accessed on December 1, 2017, 7.

21. Defined here in U.S. military doctrine as: *"Cyberspace Operations are composed of the military, intelligence, and ordinary business operations of DOD in and through cyberspace . . . The successful execution of CO requires the integrated and synchronized employment of offensive, defensive, and DODIN operations, underpinned by effective and timely operational preparation of the environment. CO missions are categorized as offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), and DODIN based on their intent. OCO are CO intended to project power by the application of force in and through cyberspace. DCO are CO intended to defend DOD or other friendly cyberspace. DODIN operations are actions taken to design, build, configure, secure, operate, maintain, and sustain DOD communications systems and networks in a way that creates and preserves data availability, integrity, confidentiality, as well as user/entity authentication and non-repudiation."* U.S. Joint Staff, (2013, February 3), ***Cyberspace Operations*** (Joint Publication 3-12(R)), vii. It is interesting to note that in testimony to the House Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities in May 2017, CYBERCOM Commander Admiral Rogers' assessment of the "Cyber Threat Environment" only one sentence or less than 4% of the text was devoted to state-sponsored information influence campaigns with no mention of the Russian influence campaign. By contrast, nearly 20% of the assessment was devoted to the non-state ISIS influence campaign, with the remaining 75% of the threat assessment being devoted to threats to cyber networks and systems, https://armedservices.house.gov/legislation/hearings/fiscal-year-2018-budget-request-us-cyber-command-cyber-mission-force-support, accessed on December 1, 2017.

22. Defined here in U.S. military doctrine as: "Information Operations as the integrated employment, during military operations, of Internet-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. U.S. Joint Staff (2014, November 20) ***Information Operations*** (Joint Publication 3-13), ix.

23. Susan L. Gough, (2003, April 7), ***The Evolution of Strategic Influence*** (Carlisle Barracks, PA, U.S. Army War College, USAWC Strategy research Project), 1.

24. Even Department-level strategy documents, most particularly the Department of Defense Strategy for Operations in the Information Environment, https://www.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf, accessed on October 15, 2017, contain "operations" to a military operational context focused around supporting Joint Force Commanders. While similar references occur in most doctrine statements, and take as an example, the U.S. Marine Corps definition of information operations: "Information Operations is the integration, coordination and synchronization of all actions take in the information environment to affect a target audience's behaviour in order to create an operational advantage for the commander", http://www.quanitco.marines.mil/Tenants/Marine-Corps-Information-Operations-Center/, accessed on October 15, 2017.

25. Narrative power defined *"...a vehicle for manipulating individuals so that they are more inclined to do what you want, not because you have forced them to but because you have convinced them that they want to do what you want them to."* (Brandon R. Allenby (2017, Summer) "The Age of Weaponized Narrative or Where Have You Gone, Walter Cronkite?" ***Issues in Science and Technology,*** 66, http://issues.org/33-4/the-age-of-weaponized-narrative-or-where-have-you-gone-walter-cronkite/, accessed on September 10, 2017.

26. Peter Roberts, (2017, February/March) "Designing Conceptual Failure in Warfare – The Misguided Path of the West" RUSI Journal, 162, 1, 18.

27. For a treatment of all the different sources of soft power, see Giulio M. Gallarotti, (2015), "Smart Power: Definitions, Importance and Effectiveness" ***Journal of Strategic Studies*** 38:3, 249.

28. Mark Leonard, (2016, January) "Weaponising Interdependence" in Mark Leonard (ed.), ***Connectivity Wars – Why Migration, Finance and Trade are the Geo-Economic Battlefields of the Future*** (European Council on Foreign Relations), 13, http://www.ecfr.eu/europeanpower/geoeconomics, accessed on November 7, 2017.

29. U.S. Department of Defense, (2015), ***The Department of Defense Cyber Strategy,*** Washington D.C., https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy/, accessed on November 30, 2017.

30. See for example: Samanth Subramanian, (2017, February), "Inside the Macedonian Fake News Complex" ***Wired Magazine,*** https://www.wired.com/2017/02/veles-macedonia-fake-news/, accessed on October 24, 2017; Samantha Bradshaw and Philip Howard (2017) ***Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation*** (Oxford, Oxford Internet Institute, Computational Propaganda Research Project Working Paper 12), http://comprop.oii.ox-.ac.uk/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf, ccessed on August 12, 2017; Andrei

Soldatov, (2017, February-March) "Putin's Private Hackers' ***The World Today*** (London, Chatham House), https://www.chathamhouse.org/system/files/publications/twt/Putin%E2%80%99s%20private%20hackers%20Soldatov.pdf, accessed on June 12, 2017; Keir Giles, (2015, August-Sept) "Putin's Troll Factories" The World Today Vol. 71, No. 4 (London, Chatham House), https://www.chathamhouse.org/publication/twt/putins-troll-factories, accessed on 12 October 12, 2017, Nichole Einbeinder, (2017, November 1), "The Election is Over, But Russian Disinformation Hasn't Gone Away" PBS Frontline, https://www.pbs.org/wgbh/frontline/article/the-election-is-over-but-russian-disinformation-hasnt-gone-away/, accessed on November 12, 2017.

31. Nazli Choucri, (2012), ***Cyberpolitics in International Relations*** (Cambridge Mass, MIT Press), 4.

32. Bernard Brodie, (1959), Strategy in the Missile Age (Santa Monica, The Rand Corporation, Report R-335).

33. Clayton Christensen, (2013), ***The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail*** (Cambridge, Mass., Harvard Business Review Repress, Reprint Edition).

34. This is seen, for example, in the Obama Administration's "Third Off-set Strategy", confirmed in mid-2017 in the Office of Management and Budget Memorandum on R&D priorities for FY 2019. The third offset strategy was designed to "'offset' potential competitors as they reach parity with the United States in some critical area." It was established to recognize that; "Adversaries are devising ways to counter our technological over-match. So across the board, we see rapid developments in nuclear weapons, modernization of nuclear weapons, new anti-ship, anti-air missiles; long-range strike missiles; counter-space capabilities; cyber capabilities, electronic warfare capabilities; special operations capabilities that are operated at the lower end. All are designed to counter our traditional military strengths and our preferred way of operating." Pellerin, Cheryl, (2016, October 31), "Deputy Secretary: Third Offset Strategy Bolsters America's Military Deterrence" ***DoD News,*** U.S. Department of Defense, Defense Media Activity), https://www.defense.gov/News/Article/Article/991434/deputy-secretary-third-offset-strategy-bolsters-americas-military-deterrence/, accessed on November 30, 2017; Also see: U.S. Office of Management and Budget Memorandum (2017, August 17), FY 2019 Administration Research and Development Budget Priorities (M-17-30), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-30.pdf, accessed on November 30, 2017.

35. Xenios Thrasyvoulou, (2014, December), "Understanding the Innovator's Dilemma" Wired Magazine, https://www.wired.com/insights/2014/12/understanding-the-innovators-dilemma/, accessed on November 30, 2017.

36. Christopher Paul and Miriam Matthews, (2016) ***The Russian "Firehose of Falsehood" Propaganda Model Why It Might Work and Options to Counter It*** (Santa Monica CA, Rand Corporation PE-198-OSD), https://www.rand.org/pubs/perspectives/PE198.html, accessed on August 3, 2017.

37. Alexander Klimberg, (2017, July), ***The Darkening Web – The War for Cyberspace*** (New York, Penguin Press), 2; Council on Foreign Relations Fellow, Gordon Goldstein summarized Klimberg's view: the ". . . internet has become an arena for [an]...international security competition fought in an increasingly Hobbesian ecosystem of digital aggression and overt information warfare." Gordon M. Goldstein, (2017, August 4), "How Enemy States do Battle in Cyberspace" Washington Post Book Review, https://www.washingtonpost.com/opinions/how-enemy-states-do-battle-in-cyberspace/2017/08/04/0bb43914-672f-11e7-8eb5-cbccc2e7bfbf_story.html?utm_term=.01e76da8a88b, accessed on October 10, 2017.

38. Barack Obama, (2015) ***National Security Strategy*** (Washington D.C. The White House), https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf, accessed on August 10, 2017, 8.

39. Braden R. Allenby, (2017, Summer), "The Age of Weaponized Narrative or Where Have You Gone, Walter Cronkite?" ***Issues in Science and Technology,*** 66, https://weaponizednarrative.asu.edu/publications/age-weaponized-narrative, accessed on September 24, 2017. This fits with the Russian Ministry of Defence's 2011 Conceptual Views on the Activities of the Armed Forces of the Russian federation in Information Space, quoted by Timothy Thomas, as active measures to: "undermine political, economic and social systems, carry out mass psychological campaigns against the population of a State in order to destabilize society and the government; and force a State to make decisions in the interests of their opponents." Thomas, Timothy, (2016, February 17) "Russia's 21st Century Information War: Working to Undermine and Destabilize Populations" Defence Strategic Communications Vol. 1, 11, https://www.stratcomcoe.org/timothy-thomas-russias-21st-century-information-war-working-undermine-and-destabilize-populations, accessed on 4 April 2017. In this, Russian strategists have taken a leaf from war-strategist Sun Tzu's axioms, most particularly: *(1) supreme excellence consists in*

breaking the enemy's resistance without fighting; (2) You can be sure of succeeding in your attacks if you only attack places which are undefended; and (3) If your enemy . . . is temperamental, seek to irritate him. Pretend to be weak, that he may grow arrogant . . . If his forces are united, separate them. If sovereign and subject are in accord, put division between them. Attack him where he is unprepared, appear where you are not expected." See https://suntzusaid.com/, accessed on December 2, 2017; and Eric Jackson, (2014, May 23), "Sun Tzu's 31 Best Pieces of Leadership Advice" ***Forbes Magazine,*** https://www.forbes.com/sites/ericjackson/2014/05/23/sun-tzus-33-best-pieces-of-leadership-advice/#748c2eaa5e5e, accessed on December 2, 2017.

40. Brad Allenby, (2017, June), "What's New About Weaponized Narrative? White Paper for the U.S. National Academy of Sciences" (Arizona State University, Weaponized Narrative Initiative), https://weaponizednarrative.asu.edu/publications/weaponized-narrative-white-paper-0, accessed on September 12, 2017.

41. For example, in Charles Kriel's review essay, he notes: *"According to Grassegger and Kroegerus, Cambridge Analytica divided America into 32 personality types for the Trump Campaign, and focused on seventeen states . . . The company's psychometric findings told the Trump Team which messages were working and where . . . One hundred-and-seventy-five thousand algorithmically-generated variations were designed not only to get out the vote, but to suppress it as well."* [emphasis added] Charles Kriel, (2017, Autumn), "Fake News, Fake Wars, Fake Worlds" ***Defence Strategic Communications*** 3, https://www.stratcomcoe.org/charles-kriel-fake-news-fake-wars-fake-worlds, accessed on December 2, 2017). See also: Illing, Sean (2017, Oct 22), "Cambridge Analytica, the Shady Data Firm that Might be a Key Trump-Russia Link, Explained), https://www.vox.com/policy-and-politics/2017/10/16/15657512/cambridge-analytica-trump-kushner-flynn-russia, accessed on October 22, 2017). See also Nicholas Fandos, Cecila Kang, Mike Isaac (2017, November 1), "House Intelligence Committee Releases Incendiary Russian Social Media Ads." ***New York Times,*** https://www.nytimes.com/2017/11/01/us/politics/russia-technology-facebook.html, accessed on November 4, 2017. Also in this context can be considered the Twitter posts that were designed to gull voters into believing that sending a text message would record their vote. This voter suppression tactic was revived in the late 2017 Virginia Gubernatorial election. O'Sullivan, Donnie (2017, November 8), "Virginia Voter Suppression Tweets went Undetected by Twitter for Hours, http://money.cnn.com/2017/11/07/media/twitter-virginia-voter-suppression/index.html, accessed on December 2, 2017.

42. Simon Kemp (2017, January 24), ***Digital in 2017: Global Overview*** (WeareSocial.Hootsuite), https://wearesocial.com/special-reports/digital-in-2017-global-overview, accessed on December 2, 2017.

43. Pew Research Center (2017, January 12) ***Social Media Fact Sheet,*** http://www.pewinternet.org/fact-sheet/social-media/, accessed on 12 August 2017; and Elisa Shearer and Jeffrey Gottfried, (September 1, 2017), ***News Use Across Social Media Platforms 2017*** (Pew Research Center), http://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/, accessed on September 30, 2017.

44. See https://intelligence.house.gov/calendar/eventsingle.aspx?EventID=814, accessed on November 22, 2017, and Kathleen Chaykowski (2017, October 31) "Highlights From Facebook's, Twitter's First Senate Hearing On Russian Meddling" ***Forbes Magazine,*** https://www.forbes.com/sites/kathleenchaykowski/#4f136f241ea1, accessed on November 10, 2017.

45. Issie Lapowsky, (2017, November 1), "Eight Revealing Moments from the Second Day of Russia Hearings ***Wired Magazine,*** https://www.wired.com/story/six-revealing-moments-from-the-second-day-of-russia-hearings/, accessed on November 10, 2017.

46. See for example: Senate Armed Services Subcommittee on Cybersecurity, (2017, April 27), ***The Weaponization of Information – the Need for Cognitive Security*** (Testimony: Rand Waltzman), CT-473, Senate; and Kelly Born, (2017, October 9) "Six Features of the Disinformation Age" ***Stop Fake,*** https://www.stopfake.org/en/six-features-of-the-disinformation-age/, accessed on December 2, 2017.

47. See for example, Seth Flaxman, Sharad Goel, Justin M. Rao, (2016) "Filter Bubbles, Echo Chambers and Online News Consumption" ***Public Opinion Quarterly,*** 80, Special Issue, 298–320; and Freedom House, (2017, November 9) ***Freedom on the Net 2017 – Manipulating Social Media to Undermine Democracy,*** https://freedomhouse.org/report/freedom-net/freedom-net-2017, accessed on December 2, 2017.

48. Keir Giles, (2016, May 20), "The Next Phase of Russian Information Warfare" ***Defence Strategic Communications,*** https://www.stratcomcoe.org/next-phase-russian-information-warfare-keir-giles, accessed on April 4, 2017.

49. See for example, Bob Schieffer with H. Andrew Schwartz, (2017) ***Overload – Finding the Truth in Today's Deluge of News*** (Lanham MD, Rowman and Littlefield, Center for Strategic and International Studies).

50. Christophe Paul and Miriam Matthews, The Russian "Firehose of Falsehood" Propaganda Model Why It Might Work and Options to Counter It" ***Rand Perspectives,*** http://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf, accessed on November 12, 2017.

51. See Tom Becka's Ted Talk, (2017, March 14) ***The Real News about Fake News,*** https://www.youtube.com/watch?v=U-w6QdzUupvo, accessed on September 27, 2017, where he remarks: *"It's easier to fool someone than to convince them they were fooled."* And *"How easy it is to make people believe a lie . . . And how hard it is to undo that work again."*

52. Pew Research Center, (October, 2017) "The Partisan Divide on Political Values Grows Even Wider", http://www.people-press.org/2017/10/05/the-partisan-divide-on-political-values-grows-even-wider/, accessed on December 3, 2017.

53. Tim Wu, (2016) ***The Attention Merchants – The Epic Scramble to get Inside Our Heads*** (New York, Knopf).

54. See for example, Bryan Gardiner, (2015, December 18), "You'll Be Outraged at How Easy it was to Get You to Click on This Headline" ***Wired Magazine,*** https://www.wired.com/2015/12/psychology-of-clickbait/, accessed on November 9, 2017.

55. See for example, Julio Reis, Fabricio Benevenuto, Pedro O.S. Vaz de Melo, Raquel Prates, Haewoon Kwak and Jisun An, (2015, April 6) "Breaking the News: First Impressions Matter on Online News" Paper presented to the 2015 International AAAI Conference on Web and Social Media, https://arxiv.org/abs/1503.07921, accessed on November 12, 2017; and Emillio Ferrara and Zeyao Yang, (2015, November 6), "Measuring Emotional Contagion in Social Media" PLoS One 10 (11), http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0142390, accessed on November 12, 2017.

56. Hunt Allcott and Matthew Gentzkow (2017) ***Social Media and Fake News in the 2016 Election*** (National Bureau of Economic Research, Working Paper No. 23089), http://www.nber.org/papers/w23089, accessed on October 9, 2017, 3.

57. See for example, Ben Nimmo and Nika Aleksejeva, (2017, March 23), "Busting Fakes, Kremlin Style (Part 1) Fact checking the Russian Foreign Ministry's "fakes" page" The Atlantic Council, Digital Forensic Research Lab, https://medium.com/dfrlab/busting-fakes-kremlin-style-part-1-6bc4369d89e3, accessed on December 2, 2017.

58. See for example, Daniel Drezner, (2017) ***The Ideas Industry: How Pessimists, Partisans, and Plutocrats are Transforming the Marketplace of Ideas*** (Oxford, Oxford University Press), and Peter Overby (2017, September 20), "Who Controls Think Tanks? Shift In Funding Highlights Changes In The Industry" ***National Public Radio,*** https://www.npr.org/2017/09/20/551364067/who-controls-think-tanks-shift-in-funding-highlights-changes-in-the-industry, accessed on December 4, 2017.

59. See for example, Portia Roelofs and Max Gallien (2017, September 19) "Clickbait and impact: how academia has been hacked," http://blogs.lse.ac.uk/impactofsocialsciences/2017/09/19/clickbait-and-impact-how-academia-has-been-hacked/, accessed on November 24, 2017.

60. John C. Camillus, (2008, May) "Strategy as a Wicked Problem" ***Harvard Business Review,*** https://hbr.org/2008/05/strategy-as-a-wicked-problem, accessed on December 14, 2017.

61. The Smith-Mundt Act of 1948, amended in 1972 and 1998, prohibits the US government from "propagandizing" the American public with information and psychological operations directed at foreign audiences; some modifications have been made in President Reagan's NSD-77 in 1983, President Clinton's PDD-68 in 1999, and President Bush 43's NSPD-16 in July 2002.

62. Alexander Klimberg, (2017, July), ***The Darkening Web – The War for Cyberspace*** (New York, Penguin Press), 3.

63. Peter Diamandis, (2016, November 7) "5 Big Tech Trends that will make this Election Look Tame" ***Singularity Hub,*** https://singularityhub.com/2016/11/07/5-big-tech-trends-that-will-make-this-election-look-tame/#sm.00000wnbp-0mo1ve50u4pupplbcucw, accessed on November 12, 2017; see also, Lee Rainie and Janna Anderson, (2017, February 8), ***Code Dependent: pros and Cons of the Algorithm Age*** (Pew Research Center, http://www.pewinternet.org/2017/02/08/code-dependent-pros-and-cons-of-the-algorithm-age/), accessed on November 12, 2017.

64. See for example, Metz, Rachel (2017, October 19), "Smartphones Are Weapons of Mass Manipulation" ***MIT Review,*** https://www.technologyreview.com/s/609104/smartphones-are-weapons-of-mass-manipulation-and-this-guy-is-declaring-war-on-them/, accessed on November 7, 2017.

65. Dirk Helbing, Bruno S. Frey, Gerd Gigerenzer, Ernst Hafen, Michael Hagner, Yvonne Hofstetter, Jeroen van den Hoven, Roberto V. Zicari, Andrej Zwitter, (2017, February 25) "Will Democracy Survive Big Data and Artificial

Intelligence?" ***Scientific American,*** https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/, accessed on 12 December 2017.

66. Liana Heitin, (2016, November 8), "Digital Literacy: An Evolving Definition" ***Education Week,*** https://www.edweek.org/ew/articles/2016/11/09/what-is-digital-literacy.html, accessed on December 15, 2017.

67. Hunt Allcott and Matthew Gentzkow (2017) ***Social Media and Fake News in the 2016 Election*** (National Bureau of Economic Research, Working Paper No. 23089), http://www.nber.org/papers/w23089, accessed on October 9, 2017, 3.