June 10, 2019

Elham Tabassi
National Institute of Standards and Technology
100 Bureau Drive, Stop 200
Gaithersburg, MD 20899

Enclosed: Technical Paper: FOCAL Information Warfare Defense Standard™ (v1.0 minus Appendix)

Dear Ms. Tabassi,

Thank you for the opportunity to submit comments in response to the National Institute of Standards and Technology's (NIST) request for information on artificial intelligence (AI) standards. We assert that NIST should work collaboratively with Federal agencies and the private sector to develop a cross sector Information Warfare (IW) Defense Standard. The enclosed technical paper supports our assertion and describes our FOCAL IW Defense Standard™, which is available for anyone to use.

More Cowbell Unlimited, Inc. is a process mining and data science firm based in Portland OR. We are developing process technologies in support of national security and industry. Our mission is to help America remain a beacon of hope and strength on the world stage.

Technological advancements are a double-edged sword. AI is a tool which promises great things for humanity, such reducing poverty and allowing creativity to flourish; however, there is a dark side which we believe must be the focal point of national security. Unsurprisingly, hunger for dominance and money are present in this discussion, too.

Feeding large hordes of private information into an AI to create a "World Brain" is plausible and provides a vehicle to project power in various ways. One way to monetize and project power from this information is through advertisements. Another way--perhaps one we are already seeing-- is through IW. As the world becomes more reliant upon information, IW boosted with weaponized AI is a major threat.

AI and Information Warfare defense technologies are closely linked. In our white paper, "Process Mining: The Missing Capability in Information Warfare," we pointed out how AI techniques such as process mining may be used by both adversaries and defenders. The white paper focuses specifically on process mining AI within the context of Reflexive Control (RC) Information Warfare (IW), which can manipulate both machine (i.e., AI) and human decision making. This is an active national security concern. For example, the Intelligence Advanced Research Projects Activity (IARPA) recently announced the Trojans in Artificial Intelligence (TrojAI) program to protect AI decision making from one very narrow subset of RC IW machine intelligence manipulation.

Your solicitation listed some major areas about which NIST seeks information. Here are some direct comments, which we hope you find useful:

- Government Prioritization: We applaud the government's focus on AI leadership and a comprehensive development of technical standards and related tools in support of reliable, robust, and trustworthy systems that use AI technologies. We implore the government to engage the private sector, marshal requisite resources, and quickly tackle these challenges.
- Lagging: Based upon our review of the literature and independent research, we assert the United States and the West in general are at significant IW-related risk. The Russian 2016 election attacks, which are in the public consciousness, are not the only efforts underway. Just

because we are not aware of ongoing efforts does not mean that we should not deploy resources now to defend the homeland.

- Challenges: Continuing from "Lagging," the United States is blissfully unaware of ongoing adversarial data collection--especially across our vast critical infrastructure. Our national challenge is to educate our entire social and corporate citizenry about IW. We need to adopt a mindset which questions data integrity continually, for such a mindset goes a significant way towards IW defense.
- Current Adoption: We are not aware of any other attempts to compile, much less adopt, a comprehensive IW Defense standard.
- Current Federal Agency Involvement: We are not aware of any Federal agencies involved in comprehensive IW Defense efforts, cross-sector or otherwise.
- Needed Federal Agency Involvement: The Federal government should work closely with the private sector--especially critical infrastructure participants--to develop a comprehensive IW Defense standard to protect America from current and growing IW threat.

In a nutshell, AI and modern IW are inextricably linked, and our peer adversaries are very likely ahead of the United States and allied partners relative to IW capability. In considering new AI standards, especially AI standards designed to protect AI infrastructure from hostile manipulation and/or develop defensive AI technologies to counter hostile AI-based IW technologies, NIST should seriously consider an IW Defense standard.

IW is not a solvable problem, but it is a manageable problem. There are many inexpensive measures organizations may take to protect themselves from IW attacks; yet, to our knowledge no comprehensive IW Defense standard exists. Given the importance of IW defense, NIST could also consider a general IW Defense standard that goes beyond AI and looks at IW in the larger context of protecting both human and machine decision making from IW attack.

More Cowbell Unlimited is standing by and ready to assistance.

John Bicknell
CEO, More Cowbell Unlimited, Inc.

FOCAL Information Warfare Defense Standard™

Authors

John W. Bicknell, Jr., More Cowbell Unlimited, Inc.
Werner G. Krebs, Ph.D., Acculation, Inc.

Background

In February 2019, The White House issued an Executive Order on Maintaining American Leadership in Artificial Intelligence (AI). The Order mandate is far reaching. Among many other things, it directs Federal agencies to ensure technical standards minimize vulnerability to attacks from malicious actors and reflect Federal priorities for innovation (Executive Order on Maintaining American Leadership in Artificial Intelligence 2019).

The information age presents vivid new security challenges related to information weaponry. For instance, Russia sowed confusion and distrust during the 2016 United States Presidential election quite effectively with micro-targeted information and disinformation campaigns (Mueller 2019). Russia's highly analytical information warfare (IW) technique combines models of decision-making processes with information attack vectors designed to exploit process weaknesses--meticulously introducing into human or machine processes data which incline the adversary toward taking an action that favors the attacker (Chotikul 1986; Thomas 2004; Bicknell and Krebs 2019).

There are many ways to harness AI in an offensive capacity to commit warfare. For example, derived models of adversaries' societies and political landscapes may be probed for weaknesses and suggest information vectors which exploit those weaknesses (Bicknell and Krebs 2019). Additionally, convincing text "spambots" could lead to hard-to-stop torrents of realistic fake text information "too dangerous to release" into the public domain (Whittaker 2019), IBM's Project Debater that has shown considerable progress in enabling machine intelligences to persuasively debate humans (which could be used, for example, to scalably convince humans to vote in a dictator), unethical marketing micro-targeting (a variation of Reflexive Control) in which AI is used in conjunction with advertising microtargeting to transmit otherwise contradictory marketing messages to unsuspecting recipients as was heavily covered in the media (Bicknell and Krebs 2019; Cambridge Analytica Scandal Raises New Ethical Questions About Microtargeting 2018; IBM Research AI - Project Debater 2018; Watson 2017), and recent concern about the potential use of AI "DeepFake" technology (DNI Worldwide Threat Assessment 2019) as a more advanced form of traditional propaganda video manipulation as seen in the viral May 2019 fake Pelosi video (Wait, is that video real? 2019).

Technological advancements are a double-edged sword. AI is a tool which promises great things for humanity, such reducing poverty and allowing creativity to flourish; however, there is a dark side which we believe must be the focal point of national security. Unsurprisingly, hunger for dominance and money are present in this discussion, too. Feeding large hordes of private information into an AI to create a "World Brain" is plausible and provides a vehicle to project power in various ways (Google and the World Brain 2013; Pomeroy and Wells 2017). One way to monetize and project power from this information is through advertisements. Another way--perhaps one we are already seeing-- is through IW. As the world becomes more reliant upon information, IW boosted enhanced with weaponized AI is a major threat (Roose 2019).

In 1996, the Defense Science Board published what may be one of the most comprehensive IW Defense touchstones available, which recommended over 50 actions designed to better prepare the Department of Defense (DoD) for this *new* [emphasis added] form of warfare (Report of the Defense Science Board Task Force on Information Warfare-Defense 1996). Since the 2016 election, Congressional and Defense leaders have pushed to strengthen our strategic IW capabilities and create a Chief Information Warfare Officer within DoD (National Defense Authorization Act 2018; SASC Wants New Chief Information Warfare Officer With Authority Over Space 2017; Wanted 2018).

Since at least 1996, studies urged government agencies to resource IW defense (Report of the Defense Science Board Task Force on Information Warfare-Defense 1996). In this technical paper, we echo these suggestions and assert that America needs to develop a comprehensive IW Defense standard in order to protect the homeland. This technical paper is structured as follows. First, we discuss IW in the context of today's international climate with peer adversaries. Next, we introduce and describe a simple IW attack and defense model. Then, we present More Cowbell Unlimited's FOCAL IW Defense Standard™ which incorporates findings and recommendations from our military and data science experience as well as the literature. The standard is available for free on the More Cowbell Unlimited website. Finally, we conclude by making a case for urgent government-resourced IW defense.

Discussion

America faces a strategic imperative to innovate and rapidly field emerging technologies to remain ahead of other technical world powers. Peer adversaries, surrogate states, non-state actors, and eroding competitive advantage (A New National Security Strategy for a New Era 2017; Mattis 2018; Section 809 Panel n.d.) necessitate all aspects of information warfare be included in this imperative.

What is information warfare?

The DoD's Joint Publication on Information Operations characterizes information operations as the integrated employment of information-related capabilities to influence, disrupt, corrupt, or usurp the decision-making of adversaries. This includes integrating intelligence and analytic methods to characterize and forecast, identify vulnerabilities, determine effects, and assess the information environment (Joint Publication 3-13 Information Operations 2014).

Information warfare is fundamentally different from cyber warfare; although, it is easy to conflate the terms. Cyber warfare consists of attacks on systems. Information warfare uses information itself as the weapon. Information warfare may be conducted in cyberspace, however (Theohary 2018; White 2018).

Though an entire DoD doctrine exists on Information Operations (Joint Publication 3-13 Information Operations 2014), IW experts assert recently that, the United States and its NATO and FVEY allies remain surprisingly uneducated and lack sufficient information about IW techniques employed by our enemies--especially Russia (Galeotti 2014; Giles, Seaboyer, and Sherr 2018; King 2018).

For example, it appears as if Russia and other adversaries use kinetic operations to support IW; conversely, the West tends to deploy information tactics to support kinetic operations. This creates a false impression in the West that, as long as there is no kinetic activity, operations in the information space are not such a serious threat (Galeotti 2014). This particularly leads to a lack of focus on pre-emptive measures such as a serious focus on investing in defending against attacks in the information space (Giles, Seaboyer, and Sherr 2018).

Reflexive Control and the Long Game

Two players in a game, speaking with one another:

> Player One: I can make you say 'red.'
> Player Two: I bet you can't.
> Player One: What color is the sky?
> Player Two: Blue
> Player One: You lose. I told you that I could get you to say 'blue.'
> Player Two: No, you lose. You told me that you would make me say 'red.'

Since the 1960s, Russia has enhanced information warfare with systematic psychological or cognitive understandings of adversary reflexive processes and continues honing the technique. Known as reflexive control (RC), this highly analytical psychological method is a means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily (or reflexively) make a predetermined decision desired by the initiator of the action (Thomas 2004). By itself, RC is not an information warfare technique; rather, it is closely aligned with cybernetics and game theory (Bicknell and Krebs 2019; Chotikul 1986; King 2018; Novikov and Chkhartishvili 2014; Thomas 2004).

More recently, Russia prefers the term "active measures" which refers to operations conducted by Russian security services aimed at influencing the course of international affairs (Mueller 2019). The United States has used the term "perception management" to mean something similar to RC; however, scholars note a large difference being in the quantifiable differences in the terms "manage" and "control" (Thomas 2004).

Much has been written about the human (or social) aspect of IW. This includes Russia's attack on the 2016 United States Presidential Elections (Mueller 2019), troll farms (arXiv 2018a; Eustachewich 2019; Kowalewski 2017; Yoder 2018), social engineering attacks (Gardner 2018), and terrorist twitter activity (Krasodomski-Jones et al. 2019). Social media-related IW and disinformation will continue undermining the American political system and act as a direct national security threat to the United States for the foreseeable future (Kowalewski 2017).

Many believe that RC is deployed primarily against human soft targets, such as society and individual influencers. While certainly true, the literature describes lesser understood information targets. For example, RC may be deployed with devastating effect against machines, information systems, and physical infrastructures (Thomas 2004). False, irrelevant, altered, untimely information, and/or overwhelming information may significantly slow or cripple critical infrastructures (CI). RC is almost assuredly being adapted into the cyber domain and being deployed against automated data-processing systems which contain significant decision-making processes (Jaitner 2016).

Noted information warfare expert, Timothy Thomas, asserts that one of the most complex ways to influence a state's information resources is by use of RC measures against the state's decision-making processes. This aim is best accomplished by formulating certain information or disinformation designed best to affect a specific information resource such as:

- "information and transmitters of information, to include the method or technology of obtaining, conveying, gathering, accumulating, processing, storing, and exploiting that information;
- infrastructure, including information centers, means for automating information processes, switchboard communications, and data transfer networks;

- programming and mathematical means for managing information; and
- administrative and organizational bodies that manage information processes, scientific personnel, creators of databases and
- knowledge, as well as personnel, who service the means of informatizatsiya [informatization]." (Thomas 2004)

Adversaries may influence the human via the machine (such as an AI agent). Decision-making is dependent upon accurate and timely intelligence; if this information is inaccurate or irrelevant or otherwise delays analysis then this may seriously cripple a decision-making process (Trojans in Artificial Intelligence 2019). Therefore, opportunities exist for false, irrelevant, or untimely information to be introduced to the human, to the machine, or to both. Mapping of decision-making patterns is an extremely challenging but still achievable task. It is the knowledge of patterns within the decision-making process that allows an adversary to insert information into the process that would ultimately allow manipulation of the decision (Jaitner 2016).

For brevity and simplicity, from this point forward, we will use "IW" as a general acronym to refer to information warfare, information operations, and perception management. We will also combine "RC" and "IW" ("RC IW") to mean "RC-enhanced information warfare," as favored by Russia and presumably part of active measures campaigns.

Vulnerabilities and Countermeasures

Our nation has sixteen CI sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof (Critical Infrastructure Sectors 2013). Much literature focuses on United States and Allied CI vulnerability and resiliency (Naval Postgraduate School Center for Infrastructure Defense n.d.; Report of the Defense Science Board Task Force on Information Warfare-Defense 1996).

The Defense Science Board Task Force on IW Defense detailed at length CI vulnerabilities. They observe that the United States has built its economy and military on a technology foundation that it does not control and which, at least at the fine detail level, it does not understand. Due to CI connectedness and interoperability, there is potential for effects to cascade through one infrastructure into other infrastructures. No one seems to know quite how, where, or when effects actually would cascade (Brafman and Beckstrom 2006; Taleb 2014); nor what the total impact might be (Report of the Defense Science Board Task Force on Information Warfare-Defense 1996).

Experts from the Naval Postgraduate School (NPS) call our nation's infrastructure "soft" and "open to surveillance and attac[k] from an enemy that could be anywhere" (Brown et al. 2006). Government agencies and American corporations--especially CI participants--must assume intelligent, persistent, and resourced adversaries are gathering intelligence in order to launch insidious and potentially devastating information warfare attacks on the homeland.

By viewing CI through the eyes of intelligent adversaries, potential vulnerabilities and system fragilities may be understood by assessing the worst case outcomes. NPS' Center for CI asserts that the key idea is to base assessments on what the adversary can do, as opposed to guesses about what the adversary wants to do. This is conservative, but prudent, and it avoids having to guess at what an opponent will do (Naval Postgraduate School Center for Infrastructure Defense n.d.).

Successful protection policies must be sufficiently flexible to cover a wide range of systems and take into account threat, both from the insider and the outsider, and must espouse a philosophy of risk management (Report of the Defense Science Board Task Force on Information Warfare-Defense 1996). The following considerations are paramount for a successful IW defense (Giles, Seaboyer, and Sherr 2018):

- Knowledge of the adversary is as important as self-knowledge
- Deterring and defeating 'hybrid war' demands local knowledge
- The relationship between the military commander and political decision-maker is of the utmost importance
- There are no 'rear areas'

IW in general, and RC in particular, is a complex operation and requires effective coordination for the long-term effect to be achieved. It may be a fragile operation that is fairly easy to counter, if target audiences are made aware of the concept, how it works, and who may be exploiting it against them (Giles, Seaboyer, and Sherr 2018). Reflexive control can be successful only under the condition that the party which is being controlled does not know about this fact. Once a controlled party (the party being attacked), becomes aware of the adversary's intentions and actions, RC can damage the controlling party (the adversary). Since after discovering a trick, the controlled party may reconstruct the intentions of its opponent (Mathematical Modeling of Reflexive Processes 2003).

Highly decentralized organizations have demonstrated remarkable resilience and survivability (Brafman and Beckstrom 2006). Like a starfish, which grows new legs, leaderless organizations are able to survive what ostensibly appear to be devastating attack. For example, the Apache American Indian Nation survived in the 19th century for decades remarkably well even as the United States expended significant resources to subdue them. Similarly, Al Qaeda survives despite many years of Coalition pressure to snuff out the terrorist organization (Brafman and Beckstrom 2006).

Financial markets can also be thought of as a tool for decision making, and market economies may be considered a decentralized decision making ecosystem; throughout history, every major empire has deployed the tool of complex financial markets to manage complex decision making tasks (Goetzmann 2017). Considerations of subtle ecosystem centralization ("systematic risk", "excessive leverage," "undercollaterization" and "excessive open interest") also apply to financial markets, sometimes witnessed in the form of catastrophic financial crises (Lewis 2015; Taleb 2014). Curiously, organizations reflexively tend to constrict or centralize during crises, which increases vulnerability and decreases resiliency (Brafman and Beckstrom 2006). The very complexity and heterogeneity of today's systems may provide a measure of protection against catastrophic failure, by not being susceptible to the same precise attacks (Report of the Defense Science Board Task Force on Information Warfare-Defense 1996). Some Fortune 500, Silicon Valley tech leaders, and national security agencies are reportedly studying how to adopt hybrid model organizations with more decentralization or modify organizational structures to decentralize during contingencies while otherwise maintaining business as usual (Starfish Leadership n.d.).

IW Attack and IW Defense Methods

Based upon the discussion, we formulate the following IW Attack and IW Defense Model, Figure 1. The model is an all-encompassing novel view of the IW landscape. It shows how attacks may be conducted

against human as well as corporate and government targets, and it suggests a defense methodology, as well.

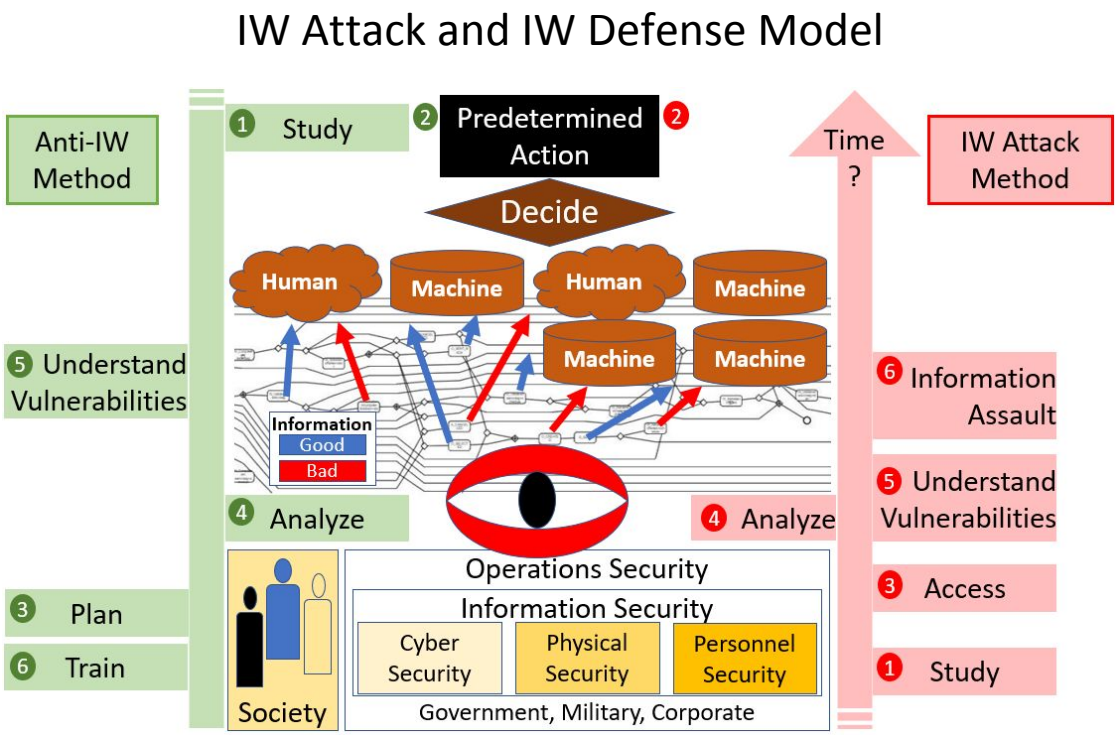

Figure 1

Model Components

Here is a brief explanation of the IW Attack and IW Defense Model components, followed by a more detailed discussion of each.

IW Attack Method: The right hand side of the model depicts a generalized process for IW attack on society or organizations upon which society depends. These elements have a red shading.

IW Defense Method: The elements on the left hand side, shaded in green, suggest IW countermeasures or an IW Defense process.

Controlled Party or Party Being Attacked: The bottom center of the model indicates that information may be used as a weapon against human or "social" targets as well as Government, Military, and Corporate targets. Notice that "Society" is completely vulnerable to IW attack. Governments and Corporations, on the other hand, have security programs which attempt to protect data.

Analysis Engine and Process Ecosystem: The center of the model displays an unbounded analysis engine which ingests and analyzes data concerning the controlled party. The goal of the analysis engine is to understand the information flow and decision making processes of the controlled party, Figure 2. Decisions may be human, machine, machine-human, or machine-machine. Once decision making processes are known, the adversary is able to infer and calculate vulnerabilities which may be exploited with clever IW attack vectors.

Information Flow and Decision Making Process

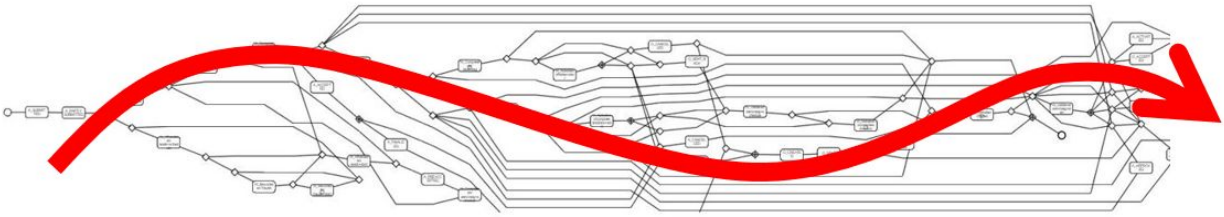

Figure 2

Decision and Predetermined Actions: The top middle portion of the model displays the controlled party's decision and predetermined action.

Model Assumptions

The model assumes adversaries will:

- breach security, despite best efforts
- access a variety of highly sensitive data
- receive tips or data from disgruntled employees, treasonous soldiers, or 'moles,' and
- use open source data to derive insights relevant to IW attack

IW Attack Method

Generalized IW attack planning and execution contains the following steps.

Time: First an important comment about Time. IW attack planning and execution time spans vary greatly. Some attacks are planned and executed quite quickly, when circumstances dictate. For example, within days after members of parliament occupied the Russian White House in October 1993, they were ousted by the Russian military by employing reflexive control, reputedly (Thomas 2004). More recently, twitter trolls sponsored by terrorist groups remained relatively dormant for months until bursts of IW activity accompanied noteworthy events (Krasodomski-Jones et al. 2019). We should expect that IW attacks on the United States, NATO, and FVEY CIs may be years in the planning.

1. Study. An attacking adversary studies the target intensely and from numerous perspectives--cultural, cognitive, operational, administrative. The adversary understands the target's market space and competitive landscape, as well as relevant historical events. This is a critical step for any successful IW attack.
2. Predetermined Action: Given the strategic, operational, and tactical landscape, the attacker decides what action he wants the controlled opponent to take. In a relatively short term attack scenario, this IW attack decision guides and informs the rest of the attack method. For longer term attack scenarios or scenarios with relatively little target data, predetermined actions may be restricted or guided by the quality or quantity of data available.
3. Access: Before an adversary may employ IW, he must have access to decision making data. The data may be any data related to the opponent or the opponent's environment. For example, it may be open source social media data, political speeches, market intelligence, emails, system log files, troop movements, etc.

4. Analyze: The adversary analyzes the data to understand decision making processes in as much detail as possible. These analyses may include reading reports or stolen documents with detailed note taking, manual process mapping, automated process ecosystem discovery, and automated organizational chart elucidation.
5. Understand Vulnerabilities: Next, the attacker uses various methods to understand social or organizational vulnerabilities into which information attack vectors may be placed in order to achieve the predetermined outcome. There are numerous manual and data-driven ways to infer vulnerabilities from process data. For example, a detailed mapping of an organization's processes may include knowledge about key decision makers, decision timing, operating hours, and the number of employees who work in various functional areas. If sufficient data have been collected, the adversary may be able to derive vulnerabilities empirically using scenario simulations and other techniques; these results may reveal areas of the business which appear overwhelmed with daily work, which contain automated decision making process elements, and organizational-level response to external stimuli. In a social context, keen manual observations gleaned from open source data reveal fault lines in cultural discourse processes which suggest vulnerability. Sophisticated empirical models of society or portions of society reveal subtle contextual information vulnerabilities which may be exploitable with clever information attacks.
6. Information Assault: The information assault may deployed in numerous ways. The assault exploits process-related vulnerabilities in such a way to incline the opponent to make a decision which favors the attacker. Given the attacker's desired effect, the data collected, and inferred vulnerabilities, the attacker decides how to deploy attack vector(s). Humans and machines receive information constantly, and this information may be true or false. In Figure 1, true information is shown as blue arrows, and false information is shown as red arrows. The information assault injects false or overwhelming information into the decision ecosystem in order to cause an outcome which favors the attacker. The attack vectors may directed at various controlled parties (see below).

IW Defense Method

1. Study. Just as an adversary studies its targets, the first step in an IW Defense is knowledge and awareness. Everyone in society must develop an awareness that information may be used as an insidious and devastating weapon; everyone should develop a skeptical mindset relative to data. This simple knowledge may be sufficient for citizens, corporations, and government agencies to thwart many IW attacks which involve human decision makers; however, businesses and governments should not stop there. They should study their respective enemies in the same level of detail the enemy is studying them.
2. Predetermined Action: Mitigating IW threat includes thinking about what the adversary might want to accomplish in an information warfare campaign against the organization. Militaries already have this mindset in an operational context. Organizations--especially CI participants--must think through possible scenarios and outcomes. Ask questions like: "What strategic decisions might I make which favor my adversary," or "What does my adversary want," or "What is my adversary's long game and how might my adversary be guiding my actions?"
3. Plan: Beyond studying, IW defense requires planning and effort--especially in a corporate or government environment. A robust and effective IW Defense program involves the entire organization as well as appropriate resourcing.
4. Analyze: Organizations need to know how information flows and how decisions are made in order to protect against information attack. Organizations must gather internal and external data in order to do a proper self-analysis. The ultimate goal is to map all corporate decision making processes. This

may be a very large undertaking. To get started, organizations may prioritize these efforts in several ways. Backward mapping is a useful technique. First, the organization may be guided based upon what the organization has learned from studying the adversary and his intentions (steps 1 and 2). Second, the organization may already have an internal physical, cyber, and information security risk matrix which might guide efforts. Finally, the organization may prioritize processes which include key corporate decisions, or processes with a very high volume of decisions.

5. Understand Vulnerabilities: Continuing along a step-wise IW Defense methodology, comprehensive defense planning identifies vulnerabilities which the adversary would likely exploit in order to achieve IW objectives. Once decision making processes are understood, there are manual and empirical methods to understand vulnerabilities. Some vulnerabilities are rather obvious. For example, people use computers and smartphones to receive information in personal and work settings; therefore, this human-to-machine interface is a vulnerability. A complicated corporate finance process or manufacturing process, if mapped explicitly, reveals vulnerabilities, as well. For example, key decision makers are susceptible to manipulation, or hackers may inject tainted data into a system which affects decisions, or sensors may be fed data which alters decisions. Red teaming efforts may also reveal critical organizational behavior vulnerabilities, such as emergency response patterns, which may be exploited by a cunning adversary. Vulnerabilities should be documented and catalogued in order to develop mitigation plans and alert people to attack possibilities. Antifragility and resilience analyses may suggest new organizational, governmental, and even societal structures which are more resilient to IW attacks.
6. Train: Plans are nothing without reinforcement and training. Organizations and societies must train themselves in order to protect against information warfare. This includes effective internal employee education, external communication protocols, and crisis/incident response plans and drills.

Controlled Party or Party Being Attacked

Controlled parties may be humans, machines, human-machine systems, or machine-machine systems. Attacks directed at humans or societies send information directly to people in order to influence decisions and actions. Strictly human IW-attacks are becoming less frequent as machines become omnipresent. Machine attacks, on industrial controls systems or programmable logic controllers for example, seek to alter automated decisions with tainted information. Human-machine attacks pass along to human decision makers information attack vectors which have first been processed through a machine; the 2016 Russian election interference which micro-targeted subsections of the population (humans) with attack vectors via a social media tech platform (machine) may be considered a human-machine IW attack. Finally, machine-machine decision making ecosystems are an emerging IW target party, an example is in the Appendix. Clearly, machines and AI are increasingly integrated with global human decision making.

Examples

See the Appendix for some IW Attack and IW Defense scenarios. (Note: This v1.0 Technical Paper is pending release of the Appendix for proprietary reasons.)

Focus IW Defense Standard™

As part of America's focus on artificial intelligence standards (Artificial Intelligence Standards 2019), organizations should adopt a comprehensive IW Defense standard. More Cowbell Unlimited's FOCAL IW

Defense Standard™ (v1.0) is available on our website for self-assessment. We also use it during client engagements to provide data science services relative to IW Defense; refer to the Appendix for some relevant scenarios. We assembled this standard based upon years of military and data science experience, and IW research (Bicknell and Krebs 2019).

"FOCAL" is an adjective which means "relating to the center or main point of interest." We believe this is highly appropriate. IW should be a national security focal point. AI advances will fuel IW capabilities which are difficult to fathom. This standard will help the nation develop an IW Defense mindset and national competency.

IW Defense Standard Assumptions

> "There are no rear areas" (Giles, Seaboyer, and Sherr 2018)

In this section, we briefly review the FOCAL IW Defense Standard™, its assumptions, and tenets, Figure 3. The standard addresses prudent IW defense activities for modern organizations. It incorporates findings and recommendations from decades of military and data science experience as well as the literature. It is a v1.0 product and will be updated periodically.

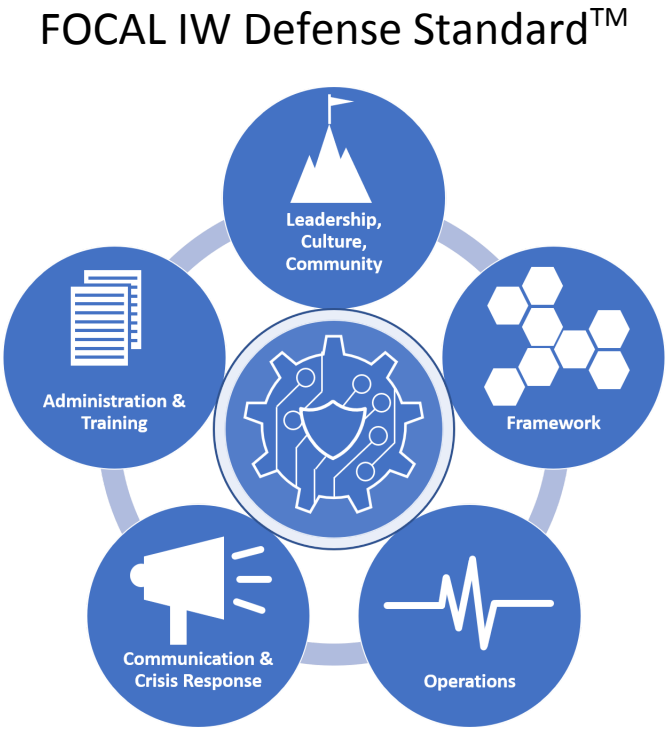

Figure 3

Assumptions

The Target: A comprehensive IW Defense tool assumes the entire homeland, its society, and CI assets are targets. We assume adversaries are playing a long game and are attempting IW which will avoid detection, until it is too late. Government and private CI participants are at great risk for insidious and devastating IW attack. Like gradually turning up the heat and boiling a frog, we hypothesize adversaries

are attempting to nudge CI participants gradually and without being detected toward a catastrophic tipping point. Adversaries may be collecting data and planning attacks which:

- Sector-specific: target a vulnerability which affects a single CI sector,
- Cross-sector: target a generalized vulnerability leveraged across multiple CI sectors,
- Insidious: cause marginal, barely noticeable, actions which favor the attacker and which have a cumulative effect over time,
- Devastating: cause a catastrophic national or international event

Integration: IW Defense is much more effective when adversaries are denied organizational emails, access to physical premises, and access to information systems. The standard, therefore, does not exist in a vacuum, but assumes organizations are also addressing physical security and cybersecurity issues within an appropriate auditable framework, such as ISO 27001, NIST Cyber Security, HiPAA/HiTrust, FIPS, DFARS, FedRAMP, etc.

Process Elucidation: Understanding processes is a fundamental IW defense component; for, it is by understanding decision making processes which enables organizations to understand and mitigate IW vulnerabilities systematically. Moreover, during the course of process documentation and vulnerability identification, users of this standard may incidentally discover substantial areas for process improvement which may be referred to continuous improvement stakeholders. For this to function properly and optimally, however, the business must have some sort of continuous process improvement framework in place, such as ISO 9001, Total Quality Management (TQM), Six Sigma and variations (Lean Six Sigma), Holacracy®, Sociocracy and variations, and specific adaptations of ISO 9001 to specific industries, such as Tkt-It for IT firms, ISO 29001 for Oil & Gas firms, etc.

Tenets

The standard is divided into five interlocking tenets. Together, these tenets help organizations, understand IW, shift culture, train the workforce, methodically identify vulnerabilities, prepare for attack, recover from attack, and contribute to the larger IW Defense community as a vested stakeholder, Figure 3.

- Framework: This standard does not exist in a vacuum. Rather, continual auditing and integration with appropriate cybersecurity and process improvement frameworks is vital for program success.
- Operations: No two organizations are the same. An effective IW Defense program consists of a strong analysis component which is customized for the organization, its competitive environment, and strategic goals. This includes red teaming with lessons learned, data driven vulnerability detection and cataloging, and resilience and antifragility analyses.
- Communication & Crisis Response: Organizations must communicate to the world and to their workforces that they are serious about IW Defense. Brand reputation and management are critical components to maintaining a growing bottomline. IW Defense crisis response plans help organizations communicate and reduce the risk before, during, and after suspected IW attacks.
- Administration and Training: Simply knowing about the possibility of IW along with relatively simple vigilance practices are a large part of an effective IW Defense program. This requires general training as well as role-specific training. Training should also be highly engaging and demand effort from the entire organization.

- Leadership, Culture, Community: Leadership from the top drives cultural shifts and is absolutely essential for effective IW Defense. Engaged executives, who lead by example and set the tone within organizations, communicate to the entire workforce how devastating IW can be to the organization, and the nation. IW is an active and creative space; leadership engagement within thought communities also demonstrates commitment to IW Defense. This tenet encourages everyone to develop an IW Defense mindset.

Other Noteworthy Features

More Cowbell Unlimited's v1.0 IW Defense standard contains the following features:

Features

- Government Modernization Initiative: In addition to the goals of the White House's Executive Order (Executive Order on Maintaining American Leadership in Artificial Intelligence 2019), our standard assists directly with several government modernization goals--specifically Data, Accountability, and Transparency, Shifting from Low-Value to High-Value Work, and IT Modernization (President's Management Agenda n.d.).
- Cross-sector and generalizable: Our standard is generalizable to all organizations--including NATO and FYEY allies.
- Trustworthiness: Our standard promotes/develops information provenance or chain of custody competencies so that systems which use AI technologies may more confidently rely upon the decision making information.
- Comprehensive: Our standard considers the entire organization and is undergoing constant refinement in support of national security.
- Leadership: One of the key tenets in our standard is "Leadership, Culture, and Community." This tenet encourages senior leaders to shift corporate culture and develop an IW Defense mindset.
- Participation and urgency: Our standard encourages corporate leaders to "lead from the front", share their experience, participate in various IW-related communities of excellence, conferences, etc.
- Broad Economic Implications: Our standard is helpful for the entire economy, potentially. In addition to IW Defense, the standard uncovers substantial areas for business process improvement, which helps the bottomline for organizations throughout America. Better business outcomes fuel the US economy.

Conclusion

Information warfare is a cognitive fight, and the United States and the West are in combat—whether we realize it or not. Decision makers must expend the resources to educate themselves and their organizations. The United States and its allies are in a precarious and vulnerable state relative to ongoing nefarious adversarial IW data collection activities and operations--especially relative to our vast CI (Brown et al. 2006; Galeotti 2014; Giles, Seaboyer, and Sherr 2018; King 2018; Report of the Defense Science Board Task Force on Information Warfare-Defense 1996). We applaud the government's focus on AI leadership and a comprehensive development of technical standards and related tools in support of reliable, robust, and trustworthy systems that use AI technologies (Artificial Intelligence Standards 2019; Executive Order on Maintaining American Leadership in Artificial Intelligence 2019). The government should marshal requisite resources and quickly tackle these challenges. Based upon our review of the literature and independent research, we assert the United States and the West in general

are at significant IW-related risk. The Russian attacks which are in the public consciousness are not the only efforts underway. Just because we are not aware of ongoing efforts does not mean that we should not deploy resources now to defend the homeland.

Historically threat actors have taken months or years to scope out targets; now, there is a decline in the duration to set up shop and take action. Process technologies enable techniques for understanding societal, cultural, political, military, and critical infrastructure process weaknesses, at scale. Algorithmic process models discovered from varieties of data augment other IW capabilities and give the West actionable, data-driven intelligence to steel against IW attack vectors (Bicknell and Krebs 2019a).

IW is not a solvable problem, but it is a manageable problem. IW Defense starts with people. Our national challenge is to educate our entire social and corporate citizenry about IW. We need to adopt a mindset which questions data integrity continually, for such a mindset goes a significant way towards IW defense. We are not aware of any other attempts to compile, much less adopt, a comprehensive IW Defense standard; nor are we aware of any Federal agencies involved in comprehensive IW Defense efforts, cross-sector or otherwise. The Federal government should work closely with the private sector--especially CI participants--to develop a comprehensive IW Defense standard to protect America from the current and growing IW threat.

More Cowbell Unlimited's FOCAL IW Defense Standard™ is divided into five interlocking tenets. Those tenets are Framework, Operations, Communications and Crisis Response, Administration and Training, and Leadership, Culture, and Community. In combination, these tenets help organizations understand IW, shift culture, train the workforce, identify vulnerabilities, prepare for and recover from attack, and contribute to the community as a vested stakeholders.

About More Cowbell Unlimited

More Cowbell Unlimited's mission is to help America remain a beacon of hope and strength. We are developing bleeding edge process technologies in support of national security and industry. We are a Service Disabled Veteran Owned Small Business.

Authors

John Bicknell is the CEO & Founder of More Cowbell Unlimited, Inc. Mr. Bicknell is a leader, lifelong learner, and passionate analytics visionary. For almost 30 years, he has helped businesses and government organizations derive actionable insights from their data, save on costs, and make more money. Before retiring from the United States Marine Corps in 2010 as a Lieutenant Colonel, Mr. Bicknell served worldwide most notably in Afghanistan and the Pentagon; he also led the "Street to Fleet" program–a process intensive human resources supply chain effort designed to discover inefficiencies, architect solutions, and repurpose manpower savings. In his corporate career, he has helped businesses derive insights from marketing, financial, human resources, and call center data. He is a member of the Military Operations Research Society and Process Analytics Expert for the International Institute for Analytics (IIA). Mr. Bicknell's Master's degree from the Naval Postgraduate School emphasizes econometrics and operations research.

Dr. Werner Krebs is CEO of Acculation, Inc. Dr. Krebs has years of industrial data science and business revenue estimation experience, highly relevant for process mining. He built and diagnosed critical financial and marketing models utilizing a wide variety of techniques: everything from classical statistics to HMM, Bayesian and traditional AI expert systems, sometimes in applications requiring ultra-low

latency or ultra-high scalability. He also generated for a technologically sophisticated high-frequency trading (HFT) hedge fund a quantifiable PnL by developing automated data-mining system to detect missing/mis-configured strategies. Dr. Krebs has been cited thousands of times in academic publications and patent applications on databases, bioinformatics, data science, statistical inference, see Google Scholar page. He has been quoted in Inc Magazine, E-Content Magazine, New York Daily News, and Science Magazine. He is a Salzburg seminar fellow and a graduate of the prestigious Founders' Institute Startup Incubator.

References

"A New National Security Strategy for a New Era." 2017. *The White House*. https://www.whitehouse.gov/articles/new-national-security-strategy-new-era/ (February 20, 2019).

"Artificial Intelligence Standards." 2019. *Federal Register*. https://www.federalregister.gov/documents/2019/05/01/2019-08818/artificial-intelligence-standards (May 14, 2019).

arXiv, Emerging Technology from the. 2018a. "Data Mining Has Revealed Previously Unknown Russian Twitter Troll Campaigns." *MIT Technology Review*. https://www.technologyreview.com/s/612252/data-mining-has-revealed-previously-unknown-russian-twitter-troll-campaigns/ (February 19, 2019).

———. 2018b. "The Tricks Propagandists Use to Beat Science." *MIT Technology Review*. https://www.technologyreview.com/s/610012/the-tricks-propagandists-use-to-beat-science/ (February 22, 2019).

Bicknell, John W, and Werner G Krebs. 2019. "Process Mining: The Missing Capability in Information Warfare." *ResearchGate*. https://www.researchgate.net/publication/331744765_Process_Mining_The_Missing_Piece_in_Information_Warfare (May 10, 2019).

"Big Data Analytics: Articles, Movies, Songs Robo-Written by Computer? « Acculation." 2014. *Acculation*. https://www.acculation.com/blog/2014/03/18/big-data-analytics-robo-generated-content/ (June 10, 2019).

Brafman, Ori, and Rod A. Beckstrom. 2006. *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations*. Penguin Books. https://www.amazon.com/Starfish-Spider-Unstoppable-Leaderless-Organizations/dp/1591841836 (May 16, 2019).

Brown, Gerald, Matthew Carlyle, Javier Salmerón, and Kevin Wood. 2006. "Defending Critical Infrastructure." *Interfaces* 36(6): 530–44.

"Cambridge Analytica Scandal Raises New Ethical Questions About Microtargeting." 2018. *NPR.org*. https://www.npr.org/2018/03/22/596180048/cambridge-analytica-scandal-raises-new-ethical-questions-about-microtargeting (June 2, 2019).

Chen, James. 2018. "Order Audit Trail System - OATS." *Investopedia*. https://www.investopedia.com/terms/o/order_audit_trail_system.asp (February 20, 2019).

Chotikul, Diane. 1986. *The Soviet Theory of Reflexive Control In...* Monterey, California: Naval Postgraduate School. http://nsarchive.gwu.edu/dc.html?doc=3901091-Diane-Chotikul-The-Soviet-Theory-of-Reflexive (February 19, 2019).

Cook, Robert. 2017. "Equity Market Surveillance Today and the Path Ahead | FINRA.Org." https://www.finra.org/newsroom/speeches/092017-equity-market-surveillance-today-and-path-ahead (February 20, 2019).

"Critical Infrastructure Sectors." 2013. *Department of Homeland Security*.

https://www.dhs.gov/cisa/critical-infrastructure-sectors (February 24, 2019).
Eustachewich, Lia. 2019. “Russian Trolls Blamed for Spreading Anti-Vaccination Propaganda.” *New York Post*. https://nypost.com/2019/02/15/russian-trolls-blamed-for-spreading-anti-vaccination-propaganda/ (February 22, 2019).
“Executive Order on Maintaining American Leadership in Artificial Intelligence.” 2019. *The White House*. https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/ (May 15, 2019).
FERC. 2016. “FERC: Industries - Smart Grid.” https://www.ferc.gov/industries/electric/indus-act/smart-grid.asp (February 20, 2019).
FINRA. 2010. “SR-FINRA-2010-044 | FINRA.Org.” http://www.finra.org/industry/rule-filings/sr-finra-2010-044 (February 20, 2019).
———. 2018a. 13 *13: How the Cloud and Machine Learning Have Transformed Market Surveillance | Episode 13*. https://embed.simplecast.com/d203ed4a?color=f5f5f5 (February 20, 2019).
———. 2018b. “FINRA Handles Record Volume of Market Activity through First Six Months of 2018 | FINRA.Org.” http://www.finra.org/newsroom/2018/finra-handles-record-volume-market-activity-through-first-six-months-2018 (February 20, 2019).
Fruhlinger, Josh. 2017. “What Is Stuxnet, Who Created It and How Does It Work?” *CSO Online*. https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html (June 5, 2019).
Galeotti, Mark. 2014. “The ‘Gerasimov Doctrine’ and Russian Non-Linear War.” *In Moscow’s Shadows*. https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/ (May 30, 2019).
Gardner, Bill. 2018. “Social Engineering in Non-Linear Warfare.” *ResearchGate*. https://www.researchgate.net/publication/326522721_Social_Engineering_in_Non-Linear_Warfare (June 2, 2019).
Giles, Kier, Anthony Seaboyer, and James Sherr. 2018. “Russian Reflexive Control.” *ResearchGate*. https://www.researchgate.net/publication/328562833_Russian_Reflexive_Control (February 19, 2019).
Goetzmann, William N. 2017. *Money Changes Everything: How Finance Made Civilization Possible*. Revised ed. edition. Princeton, New Jersey Oxford: Princeton University Press.
Google and the World Brain. 2013. https://www.amazon.com/Google-World-Brain-Brendan-Price/dp/B07K5LMFL9 (June 8, 2019).
Howard, Jacqueline. 2018. “Why Russian Trolls Stoked US Vaccine Debates - CNN.” https://www.cnn.com/2018/08/23/health/russia-trolls-vaccine-debate-study/index.html?utm_source=twCNN&utm_medium=social&utm_term=image&utm_content=2018-08-23T21%3A12%3A56 (February 22, 2019).
Huynh, Viet H., and An N. T. Le. 2012. “Process Mining and Security: Visualization in Database Intrusion Detection.” In *Intelligence and Security Informatics*, Lecture Notes in Computer Science, eds. Michael Chau, G. Alan Wang, Wei Thoo Yue, and Hsinchun Chen. Springer Berlin Heidelberg, 81–95. https://www.researchgate.net/publication/291583989_Process_Mining_and_Security_Visualization_in_Database_Intrusion_Detection.
“IBM Research AI - Project Debater.” 2018. *IBM Research AI Project Debater*. https://www.research.ibm.com/artificial-intelligence/project-debater// (June 2, 2019).
IEEE Smart Grid Big Data Analytics. 2017. “Big Data Analytics in the Smart Grid - IEEE Smart Grid.” https://smartgrid.ieee.org/resources/white-papers/big-data-analytics-in-the-smart-grid

(February 20, 2019).
"Information Warfare: What Stuxnet Hath Wrought." 2018. https://www.strategypage.com/htmw/htiw/20181208.aspx (February 23, 2019).
Jaitner, Margarita. 2016. "Applying Principles of Reflexive Control in Information and Cyber Operations." *ResearchGate*. https://www.researchgate.net/publication/311983748_Applying_Principles_of_Reflexive_Control_in_Information_and_Cyber_Operations (February 19, 2019).
Javers, Eamon. 2009. "Pentagon Preps for Economic Warfare." *POLITICO*. https://www.politico.com/news/stories/0409/21053.html (February 20, 2019).
"Joint Publication 3-13 Information Operations." 2014. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf (May 14, 2019).
King, Francis. 2018. "Reflexive Control and Disinformation in Putin's Wars." : 40.
Kirilenko, Andrei A., Albert S. Kyle, Mehrdad Samadi, and Tugkan Tuzun. 2014. "The Flash Crash: The Impact of High Frequency Trading on an Electronic Market." *SSRN Electronic Journal*. http://www.ssrn.com/abstract=1686004 (June 6, 2019).
Kowalewski, Annie. 2017. "Disinformation and Reflexive Control: The New Cold War." *Georgetown Security Studies Review*. http://georgetownsecuritystudiesreview.org/2017/02/01/disinformation-and-reflexive-control-the-new-cold-war/ (March 12, 2019).
Krasodomski-Jones, Alex et al. 2019. "Information Operations in the Digital Age." *Demos*. https://www.academia.edu/39161783/Information_Operations_in_the_Digital_Age (May 20, 2019).
Krebs, Valdis. 2002. "Uncloaking Terrorist Networks." *First Monday* 7(4). https://firstmonday.org/ojs/index.php/fm/article/view/941 (June 5, 2019).
Lewis, Michael. 2015. *Flash Boys: A Wall Street Revolt*. 1 edition. New York: W. W. Norton & Company.
Lucarelli, Fosco. 2012. "Mark Lombardi's Narrative Structures and Other Mappings of Power..." *SOCKS*. http://socks-studio.com/2012/08/22/mark-lombardi/ (June 5, 2019).
"Making DoD's Vast Logistics Enterprise More Resilient." 2019. https://www.darpa.mil/news-events/2019-05-21a (June 6, 2019).
"Mathematical Modeling of Reflexive Processes." 2003. *International Interdisciplinary Scientific and Practical Journal* 2(1). http://www.reflexion.ru/Library/EJ2003_1.pdf (May 21, 2019).
Mattis, Jim. 2018. "Summary of the 2018 National Defense Strategy." : 14.
Mishra, Ved Prakash, Yogeshwaran Sivasubramanian, and Subheshree Jeevanandham. 2017. "Detecting Attacks Using Big Data with Process Mining." *International Journal of System Modeling and Simulation* 2(2): 5.
Mueller, Robert. 2019. "Report on the Investigation into Russian Interference in the 2016 Presidential Election." : 448.
"Naval Postgraduate School Center for Infrastructure Defense." https://my.nps.edu/web/cid/our-work (May 20, 2019).
Newman, Lily Hay. 2018a. "An Elaborate Hack Shows How Much Damage IoT Bugs Can Do." *Wired*. https://www.wired.com/story/elaborate-hack-shows-damage-iot-bugs-can-do/ (June 5, 2019).
———. 2018b. "The Sensors That Power Smart Cities Are a Hacker's Dream." *Wired*. https://www.wired.com/story/sensor-hubs-smart-cities-vulnerabilities-hacks/ (June 5, 2019).
Novikov, Dmitry A., and Alexander G. Chkhartishvili. 2014. *Reflexion and Control : Mathematical Models*. CRC Press. https://www.taylorfrancis.com/books/9781315775548 (February 20, 2019).
Pomeroy, Barry, and H. G. Wells. 2017. *H.G. Wells' World Brain: Annotated with an Introduction by Barry Pomeroy, PhD*. Bear's Carvery.
"President's Management Agenda." https://www.performance.gov/PMA/PMA.html (February 21,

2019).
"Report of the Defense Science Board Task Force on Information Warfare-Defense." 1996. https://www.hsdl.org/?abstract&did= (June 1, 2019).
Roose, Kevin. 2019. "The Making of a YouTube Radical." *The New York Times*. https://www.nytimes.com/interactive/2019/06/08/technology/youtube-radical.html, https://www.nytimes.com/interactive/2019/06/08/technology/youtube-radical.html (June 8, 2019).
Samangouei, Pouya, Maya Kabkab, and Rama Chellappa. 2018. "Defense-GAN: Protecting Classifiers Against Adversarial Attacks Using Generative Models." *arXiv:1805.06605 [cs, stat]*. http://arxiv.org/abs/1805.06605 (June 5, 2019).
"SASC Wants New Chief Information Warfare Officer With Authority Over Space." 2017. https://spacepolicyonline.com/news/sasc-wants-new-chief-information-warfare-officer-with-authority-over-space/ (May 14, 2019).
Schut, Martijn. 2014. "Cyber Process Mining Ag Intelligence." http://intelligence.agconnect.nl/content/cyber-process-mining (February 20, 2019).
Section 809 Panel. "Section 809 Panel – Streamlining & Codifying Acquisition." https://section809panel.org/ (February 19, 2019).
Sheridan, Cris, Senior Editor, Co-Host, and Financial Sense. 2012. "Feedback Loops: HFT, Black-Scholes, and Cicadas." *Financial Sense*. https://www.financialsense.com/contributors/cris-sheridan/feedback-loops-black-scholes-hft-cicadas (June 10, 2019).
"Smart Grid in the United States." 2018. *Wikipedia*. https://en.wikipedia.org/w/index.php?title=Smart_grid_in_the_United_States&oldid=842280760 (February 20, 2019).
"Starfish Leadership." *Starfish Leadership*. https://www.starfishleadership.com/about (May 30, 2019).
Taleb, Nassim Nicholas. 2014. *Antifragile: Things That Gain from Disorder*. Reprint edition. New York: Random House Trade Paperbacks.
"Text - H.R.2810 - 115th Congress (2017-2018): National Defense Authorization Act for Fiscal Year 2018." 2018. https://www.congress.gov/bill/115th-congress/house-bill/2810/text/eas (May 16, 2019).
Theohary, Catherine A. 2018. "Information Warfare: Issues for Congress." *Information Warfare*: 19.
Thomas, Timothy. 2004. "Russia's Reflexive Control Theory and the Military." *The Journal of Slavic Military Studies* 17(2): 237–56.
"Trojans in Artificial Intelligence." 2019. *Trojans in Artificial Intelligence (TrojAI)*. https://www.iarpa.gov/index.php/research-programs/trojai (May 25, 2019).
"Wait, Is That Video Real? The Race against Deepfakes and Dangers of Manipulated Recordings." 2019. *USA TODAY*. https://www.usatoday.com/story/tech/2019/05/13/deepfakes-why-your-instagram-photos-video-could-be-vulnerable/3344536002/ (June 2, 2019).
"Wanted: Chief Information Warfare Officer." 2018. *SIGNAL Magazine*. https://www.afcea.org/content/wanted-chief-information-warfare-officer (May 14, 2019).
Watson, Sara. 2017. "Perspective | Russia's Facebook Ads Show How Internet Microtargeting Can Be Weaponized." *Washington Post*. https://www.washingtonpost.com/news/posteverything/wp/2017/10/12/russias-facebook-ads-show-how-internet-microtargeting-can-be-weaponized/ (February 22, 2019).
White, Ryan. 2018. "The Difference Between Cyber and Information Warfare | Crossroads Blog." https://blog.cybersecuritylaw.us/2018/02/20/the-difference-between-cyber-and-information-warfare/ (May 15, 2019).
Whittaker, Zack. 2019. "OpenAI Built a Text Generator so Good, It's Considered Too Dangerous to

Release." *TechCrunch*. http://social.techcrunch.com/2019/02/17/openai-text-generator-dangerous/ (May 29, 2019).

Worldwide Threat Assessment of the Intelligence Community. 2019. https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf (June 2, 2019).

Yoder, Kate. 2018. "Russian Trolls Shared Some Truly Terrible Climate Change Memes." *Grist*. https://grist.org/article/russian-trolls-shared-some-truly-terrible-climate-change-memes/ (February 19, 2019).

Zenko, Micah. 2015. *Red Team: How to Succeed By Thinking Like the Enemy*. 1 edition. New York: Basic Books.