2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress

Information Warfare Amplified by Cyberwarfare and Hacking the National Knowledge Infrastructure

Ronald Loui
Dept. of Computer Science / University of Illinois - Springfield
r.p.loui@gmail.com

Will Hope
US Air Force Reserve / US Department of State

***Abstract*—**This paper describes how information warfare (IW) is now being carried on the back of cyber warfare (CW). IW is thus amplified so attacks may be deeper, broader, faster, more specific, or more directly causal than in the past. The paper argues that instead of hacking an electrical grid or transportation system, disrupting operations, the new IW-on-CW strategy is a hacking of the knowledge infrastructure (KI). Causing an election-day logistics problem or spreading fake news puts the national knowledge infrastructure at risk.

Cyber attack on cyber-physical information infrastructure is traditionally biased toward the command and control of physical infrastructure. IW traditionally considers scales of time and reach appropriate to pre-internet propagation and points of failure. Critical infrastructure is considered to be power, transportation, food, water, shelter, security, and emergency response, but also communications, banking, and now, elections, news, and social media.

The next targets of national knowledge industries might be institutional or industry-wide, including engineering, education, medicine, surveillance, monitoring, investment, advertising, entertainment, and law, with new, heretofore unseen time scales. Knowledge hacking has evolved because pathways are controllable, not just perimeters breachable.

IW-on-CW is made possible by the largely voluntary surrender of epistemological checks and balances to the conveniences of cyberspace. Defenses are within the control of a vigilant population that resists trading vulnerability for convenience.

Keywords—information warfare, cyber warfare, infrastructure, knowledge, epistemology, national security, fake news, psyops

I. Introduction

Dorothy Denning's landmark work, *Information Warfare and Security* [1], was an early high point in the study of information warfare (IW) as it was being transformed by cyber warfare (CW). PSYOPS and IW had been important auxiliaries to the conduct of war for as long as strategy and tactics have existed. But CW required the advent of cyberspace, or at least automata, with programmable devices that could be usurped or altered in their processing. The internet of course put CW front and center.

Today, with “fake news” and Russian election hacking, we see attacks on the information infrastructure, not just attacks on physical infrastructure, which we already know to include (in no particular order) defense, markets, agriculture, transportation, power, health, education, safety, legal, governance, emergency response, waste, and of course, communications. These are not merely attacks on the computing that assists other functions, but on the knowledge industries and thought-formation functions of a nation.

We have made ourselves especially vulnerable to such attacks; this is the main point of this paper. It has been a voluntary adoption of epistemological vulnerability. This voluntary adoption is due to poor habits of information consumption, as well as longstanding, heretofore unexploited points of failure now fully exposed to hacking. Information infrastructure has been discussed seriously in the national security community ([2,3,4,5,6,7,8,9]) but information infrastructure has mainly been thought of as the command and control dependent on electronically programmed devices. Hence we distinguish the knowledge infrastructure from the information infrastructure.

While an inventory of IW tactics has always had broad scope, CW focus has swung between two poles. One is the “cyber Pearl Harbor” or “cyber 9/11” scenario of acute, sudden massive attack ([10,11,12,13,14,15]) that could invoke a kinetic military response. The opposite concern is chronic theft of intellectual property and inducement of higher security costs for transaction, maintenance, and monitoring, the “death by a thousand cuts” or “hundred years' cyberwar” attributed primarily to China, and calculated to taunt low-level legal and trade dispute rather than escalation to arms ([16,17,18,19]). Both are real concerns. There are myriad other concerns, e.g., regarding the intelligence, surveillance, and reconnaissance (ISR) and command, control, and communications (C3ISR/C5ISR) tactics that defense research has inventoried over several decades, especially regarding industrial control systems (ICS) and SCADA (sup. control and data acquisition) devices, CW mixed with electronic warfare (EW), forms of soft cyber power, blackmail, phishing, ransomware, etc.

This paper makes three important new observations that have emerged in the past year's rise of Russian IW-on-CW (and to a lesser extent, the recent concern over ISIS-propaganda using social networks):

1. IW amplified by CW is now about national knowledge processes, not just about usurping the command and control of physical, economic, and political systems that are connected to

978-1-5386-1956-8/17 $31.00 © 2017 IEEE
DOI 10.1109/DASC-PICom-DataCom-CyberSciTec.2017.59

information and computing technologies (ICT) through cyber-physical systems. It is IW carried on CW, or piggybacked, so CW is not merely the point of entry or even the pathway, but is the primary mechanism for an amplified IW effect, making the IW tactic deeper, broader, faster, and more consequential.

2. IW on CW takes place because knowledge industries and their information infrastructure have not been defended from intrusion at a semantic content level. National infrastructure has gotten the attention of homeland security against CW attack, but not information infrastructure against IW attack. Beyond public opinion and social decision (e.g., elections and legislation) there are many other knowledge-based activities that a nation might want to defend against IW, not just CW.

3. Hacking the information infrastructure is possible because individuals and small aggregate groups have poor epistemic defenses, born of willing dependence on single points of information failure, bottlenecked information flows, and the willful avoidance of robust dialectical processes for knowledge and decision. Individuals may not see how their own behaviors produce their society's own vulnerability.

II. IW amplified by CW

Stuxnet used CW tactics to insert malware, cross air gaps, survey computer control systems, and ultimately drive cyber-physical devices beyond their limits; meanwhile, classical information warfare used pamphlets, radios, and feints of movement for propaganda and diversion. IW-on-CW uses the ICT infrastructure to amplify or accelerate. Imagine all of the Viet Cong with loud, persistent headphones connected directly to US Operation Wandering Soul recordings (eerie noises intended to disturb enemy combatants based on their beliefs about their ancestors, which were played over loudspeakers). IW-on-CW today in some ways goes well beyond that.

Social networks and targeted email in particular provide the propagation of disinformation with faked attribution and authority. The news does not have to be “fake” so long as it has the right denial, distraction, or disruption effects, which may require only the right spin, not actual falsehoods.

ICT generally provides the potential for massive deception both in terms of sources and targets, speeds the decisionmaking and automates many entailments. It makes change easy, reduces the inertia of belief formation, and makes reversion to earlier more stable information states sometimes difficult.

Online business models seduce users into narrow sourcing of information and services, which is anathema to the diversity required to combat disinformation.

Ubiquitous and constant connection to information sources increases the epistemic attack surface.

CW permits massive reconnaissance of the specific and particular precise information, such as dossiers on personalities, tendencies, and situations, that are needed to launch highly effective IW operations. This may not always be causal, but can lead to highly predictable statistical response over a target population.

CW permits some forms of IW to be more effective due to massive reach and fast effect. For example, mass simultaneous confusion and distrust may be easy for IW-on-CW, which may not have been possible with prior IW mechanisms.

III. Knowledge Industries

Knowledge industries of concern are those where ICT are not merely facilitating, e.g., for greater efficiency or lower cost, but are in fact essential to the product. Many industries are classified by the degree or “tier” of knowledge and information technology used in the production, e.g. North American Industrial Classification System (NAICS) [20]. Each should be studied for IW-on-CW vulnerabilities. Here are a few broader areas where hacking knowledge infrastructure should be of concern.

Politics. As we have seen, voting procedures are not robust, and 50-50 winner-take-all competitions between extremes are unstable political situations, hence, easily subject to externally sourced mischief. Public opinion is manipulable over time, with CW accelerants, and so is individual opinion in many cases, if enough is known about the individual's biases and belief-formation processes.

Finance. As we have seen, markets are sensitive to rumor and sudden surprises in the news, because of automated trading, leverage, and feedback behavior among investors. The past decade is littered with examples of bank data and bank operations disruption as CW began finding targets. Flash crashes have to date been caused mainly by internal errors, not external attack. CW amplifies because there are inherent amplifiers. There are also long-term institutional reputations at risk on different time scales.

Engineering. As we have seen, engineering economics and national technological advantage depend strongly on intellectual property protection. Design and architectural engineering have long term effects that can be dirsupted by embedded mischief. Damage based on flawed data, specification, transmission, estimation, manufacture, and monitoring are concerns that pre-date CW (e.g., components out of specification). US disruption of Iranian and North Korean weapons programs are leading examples of short-term IW-on-CW CP effects. A constant inflow of errors and mistakes can ruin engineering institutions, not just engineering projects.

Medicine. We have not seen much meddling in medical knowledge processes, but domestic cyber crimes on medical records and medical devices show the way. Like any national function that depends on high-stressed, at-capacity resources and scheduling, disruption is easy if the (clearly unlawful under law of armed conflict) decision were made to target medical infrastructure. Distance medicine helps the defense; automation helps the offense. The IW here might be fear-based, and externally cultivated distrust of institutional authority (e.g., in vaccinations or ebola and zika guidelines).

Education. Like public opinion, education can be targeted by long-term IW campaigns. The blueprint is found in the self-inflicted loss of trust, loss of agreement, and movement away from center that permits knowledge infrastructure exploits (KIEs) in today's news media. Loss of the meaning of credentials and authority are similar intermediaries for disrupted national education function. A public that is willing to dispute scientists on issues like evolution and climate change

is a public willing to believe many manufactured ideas. Educational institutions that are at war with themselves over left and right extremes, that do not have a strong center, have less stabilizing effect in a society.

Law. Unlike the other knowledge industries, law is highly distributed, does not operate at cyber speeds, and is robust to error through appellate processes. Single-sources of legal data (e.g., Lexis, West, court schedules) do present hacking opportunities, as does future automation of real-time regulation compliance, which may impact industries so regulated, such as transportation. Any real-time AI system for compliance (e.g., self-driving cars) could be affected in the future. Shaking public confidence in legal outcomes would be disastrous (imagine jury nullification and militia rejection of state judicial authority cultivated by IW-on-CW campaigns).

Entertainment. Although the Sony hack showed the importance of the US entertainment industry to the economy, and the sizable effect of a single product failure on large firms, it also demonstrated the robustness of this industry to disinformation: self-inoculation due to the prevalence of rumor, innuendo, and sensational reporting. Entertainment is vulnerable to IW-on-CW not because of disruption or degradation, but through old-fashioned propaganda creation as a competing product (e.g., HERO and China's "new mainstream" or "culturally or politically uplifting" films). To the extent that the nation spends more time gaming and sharing, than watching movies in theaters, it is more vulnerable to manipulation of prejudice. News-as-entertainment and infotainment practices provide obvious targets for IW-on-CW.

IV. Epistemic Defense

The habits required to defend against IW-on-CW either:

(a) meet advanced IW attack with enhanced IW defense,

or

(b) mute the CW amplification.

Fortunately, both are entirely within the control of the individual or group that is under attack.

To enhance IW defense, some might suggest stronger habits of verification and authentication, better education in statistics and reasoning, broad readership and research before forming opinions, subjecting claims to critical analysis, dialectic, and skepticism, perhaps even higher probability thresholds for acceptance of claims. Perhaps avoiding non-robust decisions that depend on slightly tipped scales and fighting for resilient centrist majorities.

However, much of the knowledge vulnerability is self-inflicted by the narrowing of news to like-minded, partisan sources, by the casual and uncritical attribution of authority to email from acquaintances, social network posts, and pages found on the internet.

Other ways to reduce the CW effect on IW include increasing the time to decision, increasing the burden of proof, generally avoiding time-stressed reasoning and decision; avoiding single-path automation that mechanizes downstream decision-making; increasing the diversity of information-bearing sources and connections; monitoring and mirroring databases and checking for integrity of data. Perhaps we need to be more elitist and less democratic about crowd-sourced, participatory knowledge creation and revision (especially when virtual persons are part of the CW amplifier).

Outright removal of clearly mendacious cyber communications (and information contrary to a government's compelling interest) will trigger an arms race in AI, which appears to be Facebook's next step. Automatic source scoring, trusted reviewing, propagation visualization, public authority alignment, viral retransmission limits, and other information technology responses will provide active defense. So long as the population does not succumb to conspiratorial or cynical thinking, e.g., in Communist Eastern Europe when there was little access to reliable information, quality is achievable.

With the advent of internet publishing, decades ago, it seemed that the *.edu* domain would be an important arbiter of what is fact. Sadly, the attack on the authority of universities has weakened these traditional epistemic pillars.

As easy as it is to blame citizens for mental laziness and an eagerness to believe, one should also examine the business models that induce people to become cyber-dependent in the first place.

(An insightful referee pointed out that centralized or institutionalized information pillars are contrary to the crowd-sourced democratic tendencies we now see on the internet. However, the latter may be what creates many IW-on-CW opportunities. It may well be that the defense of open society against IW-on-CW resembles, in some ways, the defense of closed societies against greater openness.)

V. Role of Government

The government is not responsible for national KI defense, but should play an important role with respect to data collection and promotion of security best practices. To effectively shore up KI vulnerabilities within the public domain, there needs to exist an adequate level of information sharing between both government and industry. IW is best executed against civilian IT systems via CW [27] generally due to lower risk and lack of any type of standardized defensive framework amongst targeted organizations and personnel. Contrast this with the DoD, where extensive and dedicated counter-IW/CW units are employed, and all military personnel are required to complete annual CW and IW awareness training.

The 2015 US DoD Cyber Strategy states that KI-based targets, such as industrial control systems and medical information databases, are the emerging targets which the DoD must play a limited role in defending. Attacks on national economic or infrastructure interests directly impact the military industrial base. As the private sector controls over ninety percent of the online world, they will always be the first line of defense. In order to succeed in defensive IW-on-CW operations, the defense and intelligence communities must work in partnership with the private sector [28]. In order to facilitate enhanced protection of KIs and promote better defensive awareness, the government and industry need a framework in place which facilitates more rapid declassification and dissemination of IW-on-CW information in both directions. One area where information exchange could

be quickly enacted is shared training of cybersecurity professionals. In fact, Executive Order 3718538, signed into law in May 2017 mandates that the government support the growth and sustainment of the government and private cybersecurity workforce [28].

Per DoD doctrine, cyber operations done to further information operations focus on the incorporation of both offensive and defensive capabilities, with the goal of both to disrupt the enemy decision making process [29]. The impact of government and industry partnerships in countering IW-on-CW is important, as it follows that the defensive actions taken will ultimately, and less intuitively, influence the decision-making process of the opposition. Though increasing government and industry information sharing does bring with it concerns, such as classified information safeguarding and administrative and logistical costs, new measures must be taken to counter the swiftly evolving battle space.

VI. Conclusion

We are not alone in noticing that IW-on-CW is the cyber attack method du jour. Maj. Gen. B. Williams commented:

> The fact [that] the Russians conduct information operations leveraging cyberspace does not change the fact it is information warfare. … [T]he Russians simply leveraged the domain of cyberspace to conduct information operations more effectively than they could before cyberspace was a thing.
>
> [W]e have a population that is increasingly reliant on social media … for news and information. We are not going to wean people off those ..., so the question is: How can we conduct information operations inside our own country? … This work is not the mission of the DoD. [26]

This paper disagrees only slightly with the prescribed therapy, while in complete agreement over the diagnosis (see also [25] for earlier, similar diagnosis). Instead of government "information operations" conducted on the homeland, we focus on shoring up knowledge infrastructure defenses. The weakness was created voluntarily, by adopting epistemic habits sold as easy, convenient, and trendy ICT. A little intellectual rigor and discipline, some dialectic, some skepticism about early IT adoption, and more appreciation of the kind of intellectual infrastructure under attack would provide a lot of defense against IW-on-CW. Perhaps the people can be weaned, or at least provided with better choices.

No doubt *they* are coming for our ports and high rises and water supplies, and using cyber to get to our command and control, our grids, our DNS servers, and our switches. But with IW-on-CW, they have already been using cyberspace for denying, degrading, and disrupting our knowledge infrastructure, and we should keep this in mind too.

Acknowledgment

Eric Loui, formerly of the US State Dept, gave useful input.

Disclaimer: The views expressed are those of the authors and do not necessarily reflect the official policy or position of the Air Force, the Department of Defense, Department of State, or the U.S. Government.

References

[1] Denning, Dorothy E. *Information Warfare & Security*. Addison-Wesley, 1999.

[2] Pollitt, Mark M. "Cyberterrorism—fact or fancy?" *Computer Fraud & Sec.* 2, 1998 (1998).

[3] Anderson, Robert H., et al. *Securing the US Defense Information Infrastructure*. RAND-MR-993-05D/NSA/DARPA.1999.

[4] Sharma, Sushil K., and Jatinder ND Gupta. "Securing information infrastructure from information warfare." *Logistics Information Management* 15 (2002).

[5] Cordesman, Anthony H., and Justin G. Cordesman. *Cyber-Threats, Info. Warfare, and Critical Infrastructure Protection*. Greenwood, 2002.

[6] National Research Council. *Critical Information Infrastructure Protection & the Law*. Natl. Acad. Press, 2003.

[7] Gorman, Sean P., et al. "The revenge of distance: Vulnerability analysis of critical information infrastructure." *Journal of Contingencies & Crisis Management* 12 (2004).

[8] Cavelty, Myriam D. "Critical information infrastructure: vulnerabilities, threats and responses." *Disarmament Forum* 3 (2007).

[9] Assaf, Dan. "Models of critical information infrastructure protection." *Intl. J. of Critical Infrastructure Protection* 1 (2008).

[10] Carver Jr, Curtis A. "Information Warfare: Task Force XXI or Task Force Smith." *Military Review* 78 (1998).

[11] Miller, Jason. "Feds take 'cyber Pearl Harbor' seriously." *Homeland Security and Defense Business Council* (2007).

[12] Molfino, Emily. "VIEWPOINT: Cyberterrorism: Cyber "Pearl Harbor" is Imminent." *Cyberspaces & Global Affairs* (2012).

[13] Ewing, Philip. "Has the 'Cyber Pearl Harbor' already happened?." *DoD Buzz: Online Defense & Acquisition J.* 26 (2012).

[14] Loui, Ronald P., and Terrence D. Loui. "How to Survive a Cyber Pearl Harbor." *Computer* 49 (2016).

[15] Wirtz, James J. "The Cyber Pearl Harbor." *Intel. & Natl. Sec.* (2017).

[16] Lewis, James A. *Assessing the Risks of Cyber Terrorism, Cyber War & Other Cyber Threats*. CSIS, 2002.

[17] Knapp, Kenneth J., and William R. Boulton. "Cyber-warfare threatens corporations: expansion into commercial environments." *Information Systems Management* 23 (2006).

[18] O'Hara, Gerald. "Cyber-Espionage: A growing threat to the American economy." *Comm. Law Conspectus* 19 (2010).

[19] Taylor, Robert W., Eric J. Fritsch, and John Liederbach. *Digital Crime & Digital Terrorism*. Prentice Hall, 2014.

[20] Heckler, Daniel E. "High-technology employment: a NAICS-based update." *Monthly Lab. Rev.* 128 (2005).

[21] Quinn, James B. *Intelligent Enterprise: A Knowledge and Service Based Paradigm for Industry*. Simon and Schuster, 1992.

[22] Drucker, Peter F. "Knowledge-worker productivity: The biggest challenge." *California Man. Rev.* 41 (1999).

[23] Miles, Ian. "Services innovation: coming of age in the knowledge-based economy." *Intl. J. of Innovation Management* 4 (2000).

[24] Den Hertog, Pim, and Rob Bilderbeek. "The new knowledge infrastructure." *Services & the Knowledge-Based Economy* (2000).

[25] Hamza, Karim, and Van Dalen. "eGovernance and Strategic Information Warfare–non Military Approach." *ICIW2011: Proc. of the 6th Intl. Conf. on Info. Warfare & Sec.*, 2011.

[26] Williams, Brett T. "Cyberwarfare and information warfare must be distinguished." *C4ISRNET*, commentary April 25, 2017.

[27] U.S. Department of Defense. THE DEPARTMENT OF DEFENSE CYBER STRATEGY. Washington, D.C., 2015.

[28] Exec. Order No. 3718538, 3 C.F.R. 10 (2017).

[29] U.S. Joint Chiefs of Staff. J*oint Publication 3-13: Information Operations*. Washington, D.C., 2012.