# Content as Infrastructure: The Unlearned Lesson about Cyber Security and Information Integrity

Sean Kanuck

### *Why Content Matters*

Informational content is just beginning to be properly considered as an urgent infrastructure security concern in addition to the physical integrity and functionality of the computers and telecommunications networks that enable the transmission of such content. The 2016 and 2020 presidential elections in the United States (US) raised awareness about disinformation campaigns and greatly increased both public and private sector efforts to combat foreign influence operations. But the importance of informational content goes far beyond its potential cognitive impact on human actors, such as voters. Automated industrial control systems (ICS) and Internet of Things (IoT) devices can be adversely impacted, or even maliciously manipulated, as well. In a world of heightened reliance on artificial intelligence (AI) and/or machine learning (ML) algorithms – which require large volumes of training data – content becomes part of the infrastructure, because each datum that is processed contributes to the future functionality of the algorithm. AI/ML algorithms that are trained on or receive disinformation inputs will yield imperfect outputs.

Privately owned smartphones and IoT devices are among the many endpoints that will be dependent on AI and fifth generation telecommunications networks (5G); therefore, they – and their human users – will remain highly susceptible to the effects of false data inputs. Moreover, the compounding effects that an AI algorithm creates from any disinformation that it ingests become a genuine concern in the context of IoT, for a single error can then create cascading effects over time and across physical space. One false positive in a computer vision program could lead to the misclassification of many other objects

*All ideas stated here are solely those of the author(s) and do not reflect the positions or policies of any element of the U.S. Government.*

**Sean Kanuck** is CEO of the strategic consulting firm EXEDEC and an Affiliate of Stanford University's Center for International Security and Cooperation (CISAC). Previously, Sean served as the first U.S. National Intelligence Officer for Cyber Issues from 2011 to 2016 after a decade of experience in the CIA's Information Operations Center, including both analytic and field assignments. He was also appointed Chair of the Research Advisory Group for the Global Commission on the Stability of Cyberspace and Director of Cyber, Space and Future Conflict at the International Institute for Strategic Studies.

Sean holds degrees from Harvard University (J.D.; A.B. in Government & Philosophy), the London School of Economics (M.Sc. in International Relations), and the University of Oslo (LL.M. in Public International Law). He teaches graduate courses at George Washington University's Elliott School of International Affairs and George Mason University's Law School on artificial intelligence, national security law, and ethics.

in the future. False negatives introduced into a medical screening algorithm could impair the identification of similar life-threatening conditions in other patients. In the context of national security, automated sensing platforms, or analytic algorithms processing their data streams, that were compromised in one instance could either fail to warn of imminent danger on another occasion (i.e., false negative) or inappropriately escalate hostilities (i.e., false positive).

Whether decision makers are human beings (e.g., political leaders, military commanders, corporate executives, investors, air traffic controllers, healthcare workers, etc.) or computer programs (e.g., lethal autonomous weapons systems (LAWS), nodes on an energy grid, high-speed trading algorithms, self-driving cars, etc.), the accuracy of information is paramount for it to be actionable and trustworthy. It is also important to distinguish between the nuanced concepts of "accuracy" and "veracity" for information. The accuracy – or integrity – of information means that the data in question accurately reflects its desired or correctly inputted form; however, that does not mean such data is inherently true. Veracity, on the other hand, refers to the ultimate truth or falsehood of the data (especially as it may relate to predicting future events).

For example, a medical report could accurately enumerate the fears of a paranoid schizophrenic patient, even though such fears were ill-founded (and therefore not veracious). Similarly, a military situation report could inform a commanding officer of accurate observations, but which were actually activities designed by the adversary to mislead and deceive observing forces regarding its true intentions or maneuvers. More hypothetical scenarios will put the need for human oversight and collateral analysis into full perspective. Conceivably, a telecommunications intercept of a phone call or email could accurately report the content of that message even if the sender of the message either inadvertently or intentionally transmitted false information.

In that case, the data would meet the accuracy parameter, but the information would not meet the veracity assessment. One can also imagine a contrarian investor who bets on market positions against the "perceived wisdom" of the majority. She would want to accurately know what her counterparts believed, even if she did not place value in the veracity of their assessments. Depending on the application, veracity may be desired, but accuracy of data is always required.

***United States Cyber Doctrine***

When the United States Government (USG) began publishing its cyberspace strategic doctrine in the 1990s, it used different terminology and a much more holistic approach than it did in the early 2000s. The Department of Defense (DoD) issued Joint Pub 3-13.1 entitled "Joint Doctrine for Command and Control Warfare (C2W)" on February 7, 1996.[1] That publication presciently contextualized the actionable value of informational content:

> Information warfare (IW) capitalizes on the growing sophistication, connectivity, and reliance on information technology. The ultimate target of IW is the information dependent process, whether human or automated.[2]

Joint Pub 3-13.1 (1996) further described the military's role in the conflict over the value of information as follows:

> Command and control warfare (C2W) is an application of IW in military operations and employs various techniques and technologies to attack or protect a specific target set — command and control (C2). C2W is the integrated use of psychological operations (PSYOP), military deception, operations security (OPSEC), electronic warfare (EW), and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary C2 capabilities while protecting friendly C2 capabilities against such actions.[3]

Then, the DoD issued Joint Pub 3-13 entitled "Joint Doctrine for Information Operations" on 9 October 1998,[4] which defined offensive and defensive information operations (IO) as follows:

> Offensive IO involve the integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decision makers and achieve or promote specific objectives .... Defensive IO integrate and coordinate policies and procedures, operations, personnel, and technology to protect and defend information and information systems.[5]

In the 1990s, the DoD's emphasis was clearly on protecting the value of information and impairing or manipulating the ability of adversarial military commanders to effectively make sound decisions based on the data they were receiving. Moreover, the full range of IO and IW was understood to strategically include all elements of society that depended on modern ICTs. In his 2002 article entitled "Information Operations, Information Warfare, and Computer Network Attack: Their Relationship to National Security in the Information Age" for the U.S. Naval War College volume on "Computer Network Attack and International Law," Professor Daniel

Kuehl from the National Defense University wrote:

> The final major development shaping the new geostrategic context is the increasing reliance on computerized networks for the control and operation of key infrastructures in advanced societies. The growing reliance on these systems for the control and functioning of an increasingly large segment of the infrastructures on which we depend for economic, social, political, and even military strength is both a boon and vulnerability.[6]

In the two decades that followed the terrorist attacks on September 11, 2001, the USG and DoD took a decided turn towards a physical infrastructure security approach. Protection of physical assets – rather than informational assets – became the primary consideration and policy focus. "Homeland security" and "critical infrastructure protection" were promoted as the buzzwords for defending American interests against a new type of non-sovereign enemy that conducted sensational acts of physical violence and material destruction.

By June of 2018, the DoD's Joint Publication 3-12, entitled "Cyberspace Operations," reflected that conceptual shift to focusing on cyberspace as a vehicle (or means) for physical effect, rather than the information itself as the strategic end:

> Cyberspace operations (CO) is the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. … Relationship with the Physical Domains. Cyberspace, while part of the information environment, is dependent on the physical domains of air, land, maritime, and space. CO use links and nodes located in the physical domains and perform logical functions to create effects first in cyberspace and then, as needed, in the physical domains.[7]

The focus on cyberspace as a fifth "domain" of warfighting furthered DoD's comparison to a physical realm and distracted from the essential and abstract qualities that made IO strategically significant. By 2018, the DoD had also reached an inflection point in its strategy for engaging in cyber operations. After the revocation of President Obama's Presidential Policy Directive for cyber operations (PPD-20) by President Trump,[8] the door was open for DoD to take a more leading policy role, and its publications announced a new doctrine for persistent, tactical engagement with adversaries in cyberspace.[9] Even in light of foreign disinformation campaigns and influence operations[10] the USG sought to disable the physical and/or virtual cyber capabilities of its adversaries in lieu of engaging them in robust information warfare (IW) per se. That distinction would be akin to using terrestrial military forces to prevent an enemy's air force from taking to the sky rather than developing one's own expertise in aerial combat.

Largely owing to its commitment to liberal democracy and freedom of expression, as embodied in the First Amendment to the United States Constitution, the USG is not inclined to

perpetrate widespread disinformation campaigns. That reticence to participate in rampant IW as a modern means of force projection and coercive influence is also apparent from the diplomatic posture taken by USG representatives at United Nations (UN) working groups.[11]

***Russian Information Security Doctrine***

In marked contrast to the DoD's publications and USG submissions to the UN in recent decades, the Russian Federation has consistently highlighted the strategic significance of "information confrontation" from at least 2000.[12] In fact, Russia prefers the term "ICT" (i.e., information communication technologies) over "cyber" for that very reason. For the Kremlin, cyberspace is just a new technical means to enable national propaganda objectives that long predate the Internet, smartphones, or social media.

Russia's 2015 National Security Strategy specifically identifies "intensifying confrontation in the global information arena" as one of four key trends in international relations.[13] Moreover, Russia's 2016 Information Security Doctrine, clearly states that the "information sphere has a crucial role to play in the implementation of the strategic national priorities of the Russian Federation" and specifies several strategic objectives, including: (a) countervailing information and psychological actions; (b) suppressing ... activity detrimental to the national security of the Russian Federation; and (c) neutralizing the information impact intended to erode Russia's traditional moral and spiritual values.[14]

In its 2011 document entitled "Conceptual Views Regarding Activities of the Armed Forces of the Russian Federation in the Information Space," the Russian government defined the role of its military to include:

> To maintain the forces and means for ensuring the information security in constant readiness for repulsing the threats of military and political character in the information space ... The formation of the necessary public opinion implies its corresponding orientation and mobilization; it provides an opportunity to create in the global information space a climate promoting the limitation of the possibility for the perpetration by the organizers of the conflict of any further escalation steps.[15]

These strategic concepts have been formulated into an actionable hybrid warfare doctrine that is often (and perhaps erroneously) attributed to the Russian General Valery Gerasimov.[16]

Thus, there should be no surprise that Russia has pursued IO as an effective means of exerting coercive (as in the case of Ukraine) and meddling (as in the cases of the US and France) information operations through the strategic use of social media and disinformation. Cyberspace has provided a very effective platform for the prosecution of geographically distanced military operations aimed at destabilizing foreign governments and delegitimizing democratic institutions.

### *China's Military Doctrine*

While China's publicly available documents are less explicit – and in many cases less bellicose – than those of either Russia or the US, China's military re-organization certainly conveys its strategic perspective. The formation of the Strategic Support Force (SSF) in 2015 has co-located the People's Liberation Army (PLA) units for cyber, space, and electronic warfare.[17] This new branch will have the ability to leverage a wide range of military assets for IO objectives and pursue more integrated operations to challenge or undermine information integrity on a global level.

China's diplomatic approaches at the United Nations (UN) also underscore Beijing's policy desire to avoid formal recognition of cyber warfare with physical effects under international humanitarian law without also addressing psychological effects.[18] Rather, China has approached the issue of defending cyber infrastructures as one that is inextricably linked to regulating publicly available information. Through the Shanghai Cooperation Organisation, Beijing joined Moscow in promoting an international code of conduct for cyberspace which focuses on information security vice cyber security.[19] The authoritarian leadership in China – as in Russia – is keenly aware of the political and strategic military value of controlling informational content both within and beyond its sovereign jurisdiction.

### *Back to the Future*

The United States ushered in a new era of strategic thinking in the 1990s and then neglected it, only for its adversaries to more fully develop their own doctrines based on the same principles. Ironically, the United States and its allies are now returning to those earlier ideas as well as learning from adversarial doctrines and force structures. For example, four years after the formation of China's SSF, President Trump established the United States Space Force.[20] Beginning in 2015, the US Intelligence Community has formally highlighted the integrity of information with its potential impact on critical infrastructures (including IoT devices and AI algorithms) as a top national security concern.[21]

The last five years of DoD strategic thinking have also seen additional attention paid to the importance of information integrity in addition to the protection of physical assets for cyberspace. In particular, the June 2016 Strategy for Operations in the Information Environment (IE)[22] identifies a much more expansive end state objective: "through operations, actions, and activities in the IE, DoD has the ability to affect the decision-making and behavior of adversaries and designated others to gain advantage across the range of military operations."[23] Further, the strategy clearly articulates the ultimate goal of impacting not only the content of information, but also the beliefs and perceptions of decision makers.

> Within the IE, the United States can expect challenges across three interrelated dimensions: the physical, composed of command and control systems, and the supporting infrastructure that enables individuals and organizations to create information-related effects; the informational, composed of the content

> itself, including the manner by which it is collected, processed, stored, disseminated, and protected; and the cognitive, composed of the attitudes, beliefs, and perceptions of those who transmit, receive, respond to, or act upon information. Effects in the physical and informational dimensions of the IE ultimately register an impact in the human cognitive dimension, making it the central object of operations in the IE.[24]

That strategy was followed by a Joint Concept for Operating in the Information Environment in July 2018,[25] which elaborates on the cognitive dimension.[26]

US and UK doctrinal thinking about cyber conflict and IO is also coming full circle, albeit under the new moniker of "cyber electromagnetic activity" or "CEMA". The UK Ministry of Defence's Joint Doctrine Note 1/18 from February 2018, entitled "Cyber and Electromagnetic Activities," summarizes its approach as follows:

> CEMA must address the longstanding challenges of acquiring, using and integrating information with physical actions to create the desired effect. In addition, information and the systems which create, collect, manage and exploit this information, are critical to successful conflict outcomes. The need for CEMA coordination, coherent with a full spectrum approach and mission assurance, has escalated in recent years because of the sheer volume of information, the ease of access to it and the increasing means by which it can be exploited.[27]

***Re-Learning the Importance of Information Integrity***

It appears now that the US is catching up to its previous self, China, and Russia on the doctrinal front, and must consider the way forward. Information integrity is essential to all aspects of modern societies. The 2011 Canadian federal election witnessed one party intentionally misinform the opposing party's supporters about changes to polling locations.[28] The Syrian Electronic Army's hack of the Associated Press's Twitter account and issuance of a false tweet about President Obama's wellbeing in 2013 caused a massive redistribution of wealth in the US financial markets.[29] In India, fake news propagated via social media has repeatedly been the impetus for sectarian violence and mass migrations.[30]

Each of these cases demonstrates how inaccurate data undermines the value of information, impairs the reliability of information sources, and/or erodes public trust and confidence. To maintain critical infrastructures in today's world, one must build resiliency not only of physical installations, but also of information resources. The mastery of the Russian GRU's interference in the US presidential elections[31] was that the operations willfully remained below the commonly accepted threshold of "threat or use of force"[32] because they indirectly caused American voters to cast valid – but albeit possibly misguided – ballots. Had a foreign power directly manipulated the actual polling results or used physical coercion, rather than psychological manipulation to affect voters, then the USG certainly would have taken a more profound response.

The preceding examples reflect the manipulation of human actors or decision makers, yet disinformation can be equally, if not more efficacious, when found in automated algorithms. In our increasingly networked society of "smart" (and inherently vulnerable) devices, AI is making more and more decisions for humans. The ability to misinform sensors, or manipulate infrastructure nodes, could have serious, cascading effects. Information operations against ICS controllers – as has occurred in the Iranian nuclear facilities – could destabilize public energy grids. The driverless cars and data-rich roads of the newly envisioned smart cities could lead to transportation nightmares and even loss of life if those AI algorithms do not operate correctly.

### *Content as Infrastructure*

This article has argued that the USG's temporary turn away from its original strategic concept for cyber security (which fully valued the integrity of information) was deleterious. Only by conceiving the accuracy of data as a critical infrastructure element can we build genuine resilience. Errors, mistakes, misinformation, and disinformation can no longer be viewed as mere inputs that can be corrected later if needed. It may seem counterintuitive, but informational content must be viewed as infrastructure itself – not just data that is processed on infrastructure. The two can no longer be considered as indistinguishable. Content matters just as much as the systems used to transmit that content.

## CONCLUSION

Recent experiences with foreign efforts to influence democratic elections through cyber hacks and social media campaigns as well as competing accounts regarding the origin, propagation, and mitigation of the COVID-19 pandemic have irreversibly shifted US strategic thinking to devote much more attention to informational content in addition to physical infrastructure protection. This is a very good and necessary development. We must appreciate that our infrastructure comprises informational assets as well as physical assets, just as ICT networks are composed of both hardware and software. Unfortunately, by losing sight of our own strategic thinking, the US was ill-prepared to address the activities of other nations that exploited our own doctrinal publications. That missed lesson permitted serious transgressions against our civic institutions, public trust, and economic well-being during the last five years. Hopefully, the lesson learned will be more enduring this time around.

## NOTES

1. Available at JP 3_13_1 Joint Doctrine Command and Control Warfare (C2W) (iwar.org.uk).
2. See JP 3-13, Introduction, v.
3. See JP3-13, Introduction, v.
4. Daniel T Kuehl, "Information operations, information warfare, and computer network attack: Their relationship to national security in the information age," *International Law Studies* 76, no. 1 (2002), https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1400&context=ils.
5. Kuehl, "Information operations, information warfare, and computer network attack: Their relationship to national security in the information age," viii.
6. Kuehl, "Information operations, information warfare, and computer network attack: Their relationship to national security in the information age," 42.
7. JP 3-12, Cyberspace Operations, 8 June 2018 (jcs.mil), vii.
8. Mack DeGeurin, "US Silently Enters New Age of Cyberwarfare," *New York Magazine*, September, 2018, http://nymag.com/intelligencer/2018/09/us-rescinds-ppd-20-cyber-command-enters-new-age-of-cyberwar.html.
9. U.S. Cyber Command USCC, Cyber Command Vision Statement, (https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf 2018).
10. Michael N Schmitt, "Virtual Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law," *Chi. J. Int'l L.* 19 (2018).
11. Dennis Broeders, "The (im) possibilities of addressing election interference and the public core of the internet in the UN GGE and OEWG: a mid-process assessment," *Journal of Cyber Policy* (2021), https://www.tandfonline.com/doi/pdf/10.1080/23738871.2021.1916976.
12. See Putin's 2000 information security doctrine. Łukasz Dryblak, "The role and significance of Russian doctrinal documents, with particular focus on information security doctrines from 2000 and 2016," *Studia z Dziejów Rosji i Europy Środkowo-Wschodniej* 52, no. 3 (2017).
13. See discussion of the 2015 strategy. Dryblak, "The role and significance of Russian doctrinal documents, with particular focus on information security doctrines from 2000 and 2016."
14. See the 2016 doctrine. Dryblak, "The role and significance of Russian doctrinal documents, with particular focus on information security doctrines from 2000 and 2016."
15. See the 2011 document. Dryblak, "The role and significance of Russian doctrinal documents, with particular focus on information security doctrines from 2000 and 2016."
16. Eugene Rumer, *The Primakov (Not Gerasimov) Doctrine in Action - the Return of Global Russia*, Carnegie Endowment for International Peace (June 5, 2019), https://carnegieendowment.org/2019/06/05/primakov-not-gerasimov-doctrine-in-action-pub-79254.
17. Elsa B Kania and John K Costello, "The Strategic Support Force and the Future of Chinese Information Operations," The *Cyber Defense Review 3*, no. 1 (2018), https://www.jstor.org/stable/pdf/26427379.pdf.
18. Kimberly Hsu and Craig Murray, *China and international law in cyberspace* (US-China Economic and Security Review Commission, 2014), https://www.uscc.gov/sites/default/files/Research/China%20International%20Law%20in%20Cyberspace.pdf.
19. Timothy Farnsworth, "China and Russia submit cyber proposal," *Arms Control Today* 41, no. 9 (2011).
20. Kaitlyn Johnson, "Space Force or Space Corps?," *The Center for Strategic and International Studies* (June 2019), https://www.csis.org/analysis/space-force-or-space-corps.
21. ODNI, Worldwide Threat Assessment of the US Intelligence Community, February 26, 2015, 3, https://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf, ODNI, Worldwide Threat Assessment of the US Intelligence Community, February 9, 2016, 1-2, https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf.
22. Office of the Secretary of Defense DOD, DoD Strategy for Operations in the IE, (DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf 2016).
23. DOD, Short DoD Strategy for Operations in the IE, 2.
24. DOD, Short DoD Strategy for Operations in the IE, 3.

## NOTES

25. Office of the Secretary of Defense DOD, Joint Concept for Operating in the Information Environment (JCOIE), (https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf 2018).
26. DOD, Short Joint Concept for Operating in the Information Environment (JCOIE), 2-3.
27. JDN 1/18, Cyber and Electromagnetic Activities (publishing.service.gov.uk), section 1.2
28. Staff Canadian Press, "Keys facts and timeline of events surrounding the [2011] robocalls scandal," *CBS News*, August 14 2014, https://www.cbc.ca/news/politics/key-facts-in-canada-s-robocalls-controversy-1.2736659.
29. Patti Domm, "False Rumor of Explosion at White House Causes Stocks to Briefly Plunge; AP Confirms Its Twitter Feed Was Hacked," *CNBC*, April 23 2013, https://www.cnbc.com/id/100646197.
30. India blames mass exodus on Pakistan groups | Asia| An in-depth look at news from across the continent | DW | 20.08.2012.
31. Robert S. Mueller III, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election. Volumes I & II.(Redacted version of 4/18/2019)," (2019).
32. UN Charter Article 2(4).