Information Influence Operations: The Future of Information Dominance

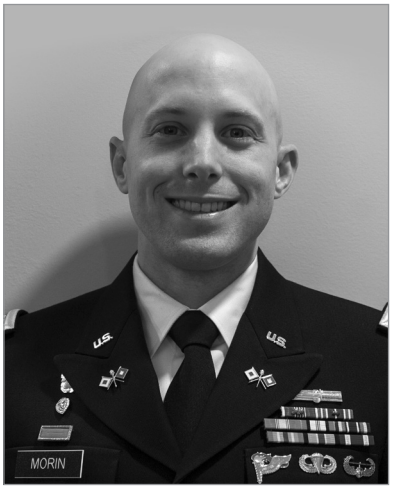
Captain David Morin

ABSTRACT

This paper proposes the development and inclusion of Information Influence Operations (IIOs) in Cyberspace Operations. IIOs encompass the offensive and defensive use of cyberspace to influence a targeted population. This capability will enable the evolution of strategic messaging in cyberspace and allow response to near peer efforts in information warfare.

INTRODUCTION

This paper proposes that Information Influence Operations (IIOs) be developed and utilized within U.S. Cyber Command's (USCYBERCOM) capability set. When correctly employed, IIOs will become a critical capability that is key to the future of cyberspace operations. IIOs must become the new "light touch", the guiding hand gently pushing public opinion, and ultimately shaping global perception and narratives in support of US strategic interests. LTG Stephen Fogarty stated: "the command [Army Cyber Command] must mimic enemy capabilities and better integrate and synchronize information operations, military deception, psychological operations, electronic warfare, all intelligence disciplines."[1] Today, most leaders consider cyber effects either an intelligence collection source or a means of causing real-world impact, such as turning off a power grid or causing significant disruption to an enemy's C2 network. Those views require revision to take full advantage of the value of cyberspace. The unrealized value of cyberspace, and what makes it so dangerous, is it allows direct access to the individual and to the public at large. This access, when used correctly, provides actors in cyberspace the ability to influence public opinion and shape the narrative of ongoing operations.



Captain David Morin is currently serving as the Company Commander of the 93d Signal Brigade Headquarters and Headquarters Company. He is from Washington, DC, and was commissioned as an officer in the Army in 2013 after earning bachelor's and master's degrees in engineering from Washington University in Saint Louis. His previous positions and assignments include Brigade Senior Network Officer (93d Signal Brigade), Battalion S6 (704th Brigade Support Battalion, 2/4ID), and Base Defense Engineer (3-62 Cavalry Squadron, 2/4ID). CPT Morin is a graduate of the Armor Basic Officer Course, the Signal Captains Career Course (SCCC), the Joint Command Control Communications and Computers Course (JC4PC), and the Joint Command Control Communications and Computers Intelligence Cyber Staff Operations Course (JC4ICSOC). He is the first signal officer to earn the Expert Soldier Badge and has also earned the Pathfinder, Airborne, and Air Assault Army qualifications and seven IT Certifications.

BACKGROUND

Unsurprisingly, senior leaders' perceptions of cyber capabilities have been shaped by popular culture and the more infamous cyber incidents and attacks. There is a plethora of apocalyptic examples of hypothetical cyber-attacks as portrayed in popular movies: *War Games* (1983), *Hackers* (1995) *Live Free or Die Hard* (2007), and *Skyfall* (2012). In all these movies, the world is nearly brought to a halt due to a single or series of cyber-attacks against military equipment, the internet or other critical infrastructure. All these fictional depictions are reinforced by reporting on some of the most well-known real-world cyberattacks such as Stuxnet, NotPetya, and the Russian actions surrounding the 2016 U.S. Presidential elections.[2] The first two of these attacks resulted in overt denial of resources and damage to equipment. Stuxnet could target almost any type of infrastructure, but was specifically designed to act against Iranian centrifuges.[3] NotPetya, a piece of ransomware with unconfirmed attribution to Russian cyber forces, was based on a leaked NSA toolkit that was substantially less targeted and as a result inflicted over $10 billion in damage worldwide as systems were rendered useless.[4] The last of these attacks, the election interference, will be the longest-lasting in its effects. "The IRA [Internet Research Agency] later used social media accounts and interest groups to sow discord in the US political system through what it termed "information warfare." The campaign evolved from a generalized program designed in 2014 and 2015 to undermine the US electoral system"[5] This offensive should be taken as a proof-of-concept in that it shows the real power of cyberspace operations, the capability to manipulate perception on a massive scale. IIOs, if developed and utilized properly, will become an incredibly powerful tool for achieving US goals in the information battlespace or even the geopolitical realm.

INFLUENCERS

As communications technology and the Internet have proliferated, capabilities previously limited to major companies and government are now accessible to anyone with an Internet connection. The traditional consumers of news can now play a major part in producing it. Bob Franklin and Lily Canter assert that "Advances in technology have profoundly impacted war reporting, affording audiences new ways in which to visualize conflict. Satellites, smartphones, laptops, and mobile broadband have enabled war reporters to communicate immediately and bring conflict live to air. Nevertheless, as new technologies open up innovative ways for journalists to convey the horrors of warfare, they similarly create opportunities for propaganda, censorship, and control."[6] The communications capabilities referenced have contributed to the creation of a power vacuum in the information realm of cyberspace. This vacuum is being filled not by traditional media and governments but by small groups of content creators and "influencers" whom have rapidly capitalized on the massive reach provided by new technologies. These "influencers" are capable of wielding influence over millions and have used this influence for a multitude of purposes from philanthropy and advertising to political ends. The future of cyber operations is the use of IIOs in cyberspace to wield influence.

The beginning of this evolution for institutional influence of information can be seen most easily through the creation and employment of state-sponsored media. While some governments have chosen to use this influence capability to maintain a well-informed public, others have begun to use the capability to explicitly influence opinion. The British Broadcasting Corporation's (BBC) mission statement is "to act in the public interest, serving all audiences through the provision of impartial, high-quality and distinctive output and services which inform, educate and entertain."[7] The BBC's mission is a prime example of the first use, simply to create a more engaged and informed populace. Its mission explicitly states that it endeavors to deliver an impartial rendering of the facts. According to recent public surveys, many believe that the BBC is effectively fulfilling this mission.[8]

In comparison, Russia Today (RT) explains its mission as: "RT creates news with an edge for viewers who want to Question More. RT covers stories overlooked by the mainstream media, provides alternative perspectives on current affairs, and acquaints international audiences with a Russian viewpoint on major global events."[9] RT admits that it is not necessarily an impartial reporter of the facts. This is important because 80% of what RT reports is factual news reporting. However, the other 20% is the part that is used more overtly to shift its audience's opinions.[10] If "unbiased" media sources continue to perform their stated mission of informing the public, they can occasionally be covertly leveraged to sway opinion or counter other sources of influence. They sway their audiences by simply continuing to report the same news and facts, but in slightly different ways. It is important to understand how organizations orient their audiences and for what purpose: to inform the public, sell more content, sow discord in a population, or spur political change.

INFLUENCE CAMPAIGNS

The future of cyber operations is to determine how to influence the public and work to regain and retain the ability to protect the narrative of our long-term strategy and vision for the world by shaping the perception of that narrative. We must develop the ability not only to dam a river, but to throw a pebble into a river and, imperceptibly but substantially, shift its flow. This subtle action must be the new paradigm for IIOs. Small imperceptible adjustments to the availability of information will enable the modification of the narrative of events seen and accepted by public opinion. This capability will enable the priming and/or shaping of public opinion to make it susceptible to US strategic messaging. Once primed, just as the pebble can either turn a smooth river into turbulent white water or direct the water slightly more left or right, so will this new form of influence operate.

Influence campaigns have already been successfully employed by our adversaries.[11] The US has been a cultural goliath since the rise of Hollywood. Now is the time for the US to leverage its dominance in the realm of ideas and transform its operational paradigm to incorporate those skills and abilities. IIOs can leverage that dominance either directly through contracting with advertising and marketing firms to create specifically targeted content, or indirectly by utilizing advertisement targeting, search engine optimization, or targeted latency. These indirect effects would allow us to effectively guide perception and even shape the targeted population's perception of reality, if effectively conducted. The ability to control a population's perception will be a critical capability in ascertaining the shape of future events and determining how actions are perceived. IIOs will be the fusion of cyberspace operations and strategic messaging.

OVERT IMPACT

In the cyber realm, the soft, unnoticed touch can be massively more impactful than the forceful haymaker. An example of an overt impact is when Amazon Inc. lost over $72 million in sales as Amazon.com went down for 63 minutes during Prime Day in 2018, a loss of over $1 million per minute.[12] Conversely, "cart abandonment," (the industry term for not completing the checkout process after adding items to an online shopping cart) due to latency, cost the e-commerce industry approximately $18 billion in 2019.[13] A 2013 study showed minor increases in latency, on the order of two seconds, increased cart abandonment rates by 30%.[14] Two seconds became the difference between a successful sale and a lost opportunity. While the cost per minute was greater during the Amazon outage, losses due to latency have had more than 200 times the impact annually. Such losses are insidious, hard to attribute, and even more difficult to fix. The fact that such minor changes in availability have such an outsized effect shows how susceptible the impatient public is to minor inconveniences.

OPERATIONALIZING IIOS

There are multiple options for making IIO's a reality. The most direct method is to take ad-

vantage of the public's need for information on demand. Even DISA defines "extreme" latency as 100ms (one tenth of a second) above normal in Mission Partner Service Level Agreements (SLAs). To take advantage of this impatience, operators need to find ways to inject a relatively small amount of lag in targeting information sources. This would be best done through indirect means such as slowing down referenced style scripts, adding slight increases to traffic (aka a low-level D/DOS, enough to slow slightly down services, but not take them down), or working at the transport layer to increase lag at key points in the routing architecture. Once that lag is in place, the operations simply need to follow up with well-targeted advertisements to offer alternative information sources. These alternative sources will have the preferred narrative that the operation seeks to advance. There is little brand loyalty in the online world. Consumers will go elsewhere to find what they need if their preference is slow or unavailable. Influencing and controlling that "someplace else" yields the opportunity to wield influence. This is possible without a great emphasis on content creation; it just requires the preferred viewpoint to be amplified and the targeted one to be dampened.

When conducted effectively, IIOs can be exceedingly powerful; however they will need to be employed in support of strong consistent national objectives to be truly effective. While IIOs can certainly be used in a short-term targeted manner, they would best be employed for long-term operations executed over the course of years to help guide long-term changes in perceptions towards US interests and preferred global structure.

IIOs need to be closely governed to ensure that, although they influence global perceptions, their impact upon domestic populations must be limited or governed appropriately. That is not to say domestic IIOs cannot be conducted, but they need to be conducted with a very different aim. The aim of domestic IIOs should be to ensure that adversarial IIOs are ineffective. This can be accomplished by utilizing news fatigue effects, exposure to more divergent views to break senses of consensus, or directly reducing the viewing of an adversary's IIO content.

CONCLUSION

IIOs offer a huge potential for advancing cyberspace operations that support US national interests without the need for large-scale deployments or use of critical offensive cyber operations capability for smaller-gain operations. However, IIOs will require a wider and longer world view for optimal employment.

IIOs represent the operationalization of cyberspace to exert influence. They provide the ability to target and influence incredibly specific, or broad, populations with targeted messaging. This influence expands the US capability to exert soft power. This soft power, represented by Information Influence Operations, facilitates economy of force in the cyber realm. Not every problem can or should be solved with force, whether that force is physical or virtual. IIOs represent the alternative. IIOs are a critical tool to be advanced by USCYBERCOM as it develops its messaging capability in the cyber domain.

DISCLAIMER

The views expressed in this work are those of the author(s) and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, or the Department of Defense.

NOTES

1. Lauren C. Williams, "Fogarty has Big Ambitions for ARCYBER." Last modified August 7, 2018, https://defensesystems.com/articles/2018/08/07/arcyber-priorities-williams.aspx.
2. Robert S. Mueller III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, Washington, DC: United States Department of Justice, 2019), 4.
3. Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon." Last modified November 3, 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.
4. Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." Last modified August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
5. Mueller, 2018, 4.
6. Bob Franklin and Lily Canter, "Digital War Reporting," *Digital Journalism Studies: The Key Concepts.* (New York: Routledge, 2019).
7. "Mission Statement," British Broadcasting Corporation (BBC), accessed February 2, 2020, https://www.bbc.com/aboutthebbc/governance/mission.
8. "BBC Report: Trust and Impartiality Nov 2017," Trust Report, British Broadcasting Corporation (BBC), last modified November 2017. https://downloads.bbc.co.uk/aboutthebbc/insidethebbc/howwework/reports/pdf/bbc_report_trust_and_impartiality_nov_2017.pdf.
9. "About Us," Mission Statement, Russia Today, accessed February 2, 2020, https://www.rt.com/about-us/.
10. "Seven Commandments of Fake News – New York Times exposes Kremlin's methods," EU vs. DisInfo, European External Action Service (EEAS), last modified November 21, 2018. https://euvsdisinfo.eu/seven-commandments-of-fake-news-new-york-times-exposes-kremlins-methods/.
11. Mueller, 2018, 4.
12. Allison Enright, "The Potential Cost of Amazon's Prime Day Miss: 72 Million," last modified July 17, 2018, https://www.digitalcommerce360.com/2018/07/17/the-potential-cost-of-amazons-prime-day-miss-72-million/.
13. Design Advisor. "Shopping Cart Abandonment Stats." Last modified March 25, 2019. https://designadvisor.net/blog/shopping-cart-abandonment-stats/.
14. Tammy Everts, "Case Study: Slow Load Times Shopping Cart Abandonment," last modified October 31, 2013, https://blog.radware.com/applicationdelivery/applicationaccelerationoptimization/2013/10/case-study-slow-load-times-shopping-cart-abandonment/.