ARMY UNIVERSITY PRESS
(http://www.armyupress.army.mil/)
Military Review
The Professional Journal of the U.S. Army
/Military-Review/)

Social Cybersecurity
An Emerging National Security Requirement

Lt. Col. David M. Beskow, U.S. Army
Kathleen M. Carley, PhD

Download the PDF (/Portals/7/military-review/Archives/English/MA-2019/Beskow-Carley-Social-Cyber.pdf)

Capt. Taiwan Veney (*center*), cyber warfare operations officer, watches members of the 175th Cyberspace Operations Group—(*left to right*) Capt. Adelia McClain, Staff Sgt. Wendell Myler, Sr. Airman Paul Pearson, and Staff Sgt. Thacious Freeman—analyze log files and provide a cyber threat update utilizing a Kibana visualization on the large data wall 3 June 2017 in the Hunter's Den at Warfield Air National Guard Base, Middle River, Maryland. (Photo by J. M. Eddins Jr., U.S. Air Force)

Social cybersecurity is an emerging subdomain of national security that will affect all levels of future warfare, both conventional and unconventional, with strategic consequences. Social cybersecurity "is an emerging scientific area focused on the science to characterize, understand, and forecast cyber-mediated changes in human behavior, social, cultural, and political outcomes, and to build the cyber-infrastructure needed for society to persist in its essential character in a cyber-mediated information environment under changing conditions, actual or imminent social cyber-threats."[1] Technology today is enabling both state and nonstate actors to manipulate the global marketplace of beliefs and ideas at the speed of algorithms, and this is changing the battlefield at all levels of war.

While recently viewed through the lens of "hybrid" warfare, information warfare is becoming an end unto itself. Dmitry Kiselev, coordinator of the Russian state agency for international news, states that "information wars are … the main type of war."[2] Information is used to strengthen your narrative while attacking, disrupting, distorting, and dividing the society, culture, and values of other competing states and organizations. By weakening trust in national institutions, consensus on national values, and commitment to those values across the international community, an actor can win the next war before it has even begun. In fact, reflecting the change from periodic conflict to continual competition, senior leaders in the Russian General Staff have claimed, "Wars are not declared but have already begun."[3]

Information is strengthening its position within the elements of national power. Strategy is often viewed through the elements of national power: diplomatic, information, military, and economic. Technology now allows state and nonstate actors to extend their power in the

information domain at a scale and complexity long thought impossible. If left unchecked, this emerging "information blitzkrieg" will have strategic effects on par with the physical blitzkrieg unleashed at the outset of World War II.

While technical in nature, social cybersecurity differs from traditional cybersecurity. Traditional cybersecurity involves humans using technology to "hack" technology. The target is information systems. Social cybersecurity involves humans using technology to "hack" other humans. The targets are humans and the society that binds them. This twist on the traditional cyber paradigm is sometimes referred to as "cognitive hacking." While leveraging the cyber medium for mass delivery, this emerging information warfare leverages advances in targeted (or micro) marketing, psychology and persuasion, policy gaps at and between private and government institutions, and understanding of the social sciences to deploy coordinated information operations with strategic effect.

Social cybersecurity is inherently multidisciplinary computational social science. "Emerging theories blend political science, sociology, communication science, organization science, marketing, linguistics, anthropology, forensics, decision science, and social psychology."[4] Many researchers in this field are leveraging computational social science tools such as network analysis, spatial analysis, semantic analysis, and machine learning. These are applied at multiple levels, from the individual through the conversation level to the larger community level.

If left unchecked, this emerging 'information blitzkrieg' will have strategic effects on par with the physical blitzkrieg unleashed at the outset of World War II.

”

In order for the Department of Defense (DOD) “to defend the security of our country and sustain American influence abroad,” our military leaders must understand this emerging discipline of social cybersecurity and how it impacts our force, nation, and values.[5] This article will introduce and define this emerging discipline, briefly discuss its history and the sociotechnological changes that enable it, and finally discuss current and emerging social cybersecurity “forms of maneuver.” Throughout this process, we will elaborate on the similarities and differences between social cybersecurity and traditional cyber operations.

Backdrop: Russian Information Blitzkrieg

Russia is waging the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare.

—Gen. Philip Breedlove, NATO Wales Summit 2014[6]

The Russian propaganda apparatus, long directed at its own society as well as the satellite states of the former Soviet Union, is now aiming at targets abroad. In 2013, Gen. Valery Gerasimov identified information warfare as an important aspect of Russian warfare going forward in his now famous article, “The Value of Science is in the Foresight.”[7] While the West viewed the article backward through the lens of the Ukrainian conflict and has arguably misattributed it as the start of hybrid warfare for Russian armies, his article was in reality his perspective of the Arab Spring as well as U.S. operations in Yugoslavia, Iraq, and Afghanistan.[8] In Gerasimov’s view, the Arab Spring and the U.S.-led coalitions in the Middle East relied heavily on resources other than conventional military forces to shape events, especially information operations. Military forces were only introduced at the last minute as a coup de grâce.

Having studied these conflicts, he sought to accelerate ongoing information warfare initiatives, stating, “Information warfare opens wide asymmetric possibilities for decreasing the fighting potential of enemy.”[9] These activities were in line with traditional Russian KGB (Committee for State Security) operations known as “active measures.” These were described by KGB Maj. Gen. Oleg Kalugin as “active measures to weaken the West, to drive wedges in

Skip to main content (Press Enter).

the Western community alliances of all sorts, particularly NATO, to sow discord among allies, to weaken the United States in the eyes of the people in Europe, Asia, Africa, Latin America, and thus to prepare ground in case the war really occurs."[10] Kalugin's quote highlights one of the critical roles of the theorized Russian information blitzkrieg, which is to drive wedges in every fissure possible, fracturing a nation or coalition. This includes driving wedges between political parties, between races, between religions, between a nation and its military, and between a nation and its allies. A fractured nation is inherently a less potent nation in terms of its ability to withstand an attack.

The emerging manifestations of Russian information operations are built on a long history of Soviet-era propaganda operations. In 1951, then Yale Law professor Harold Lasswell summarized the Soviet propaganda machine (to which the current Russian security apparatus is heir) by concluding,

> The chief strategic aim of [Soviet Propaganda] is to economize the material cost of protecting and extending the power of the Russian elite at home and abroad. Such propaganda is a struggle for the mind of man, from the Soviet point of view, only in the sense that it is a struggle for the control of the material means by which the minds of the masses are believed to be molded. Hence the purpose of Russian propaganda is not peaceful persuasion of the majority of the people in a given country as a prelude to taking power. Rather, the task is conceived as that of a minority that must remain an ideological minority until it succeeds in accumulating the material means of obtaining consensus … Soviet propagandists and their agents can lie and distort without inner restraint, for they are largely immunized from the claims of human dignity in any other sense than the dignity of … contributing to the present and future power of the Kremlin elite.[11]

This general approach continues to this day, building a small nucleus while dividing all opposing organizations and institutions, leveraging disinformation at all times. Today, however, technology enables this at a scale and distance unheard of in 1951.

The Russian state is not approaching this haphazardly. Since as early as 2003, the Russian Academy of Sciences has conducted basic research to develop advanced applied mathematical models of information warfare and its application to society. Its researchers combine social science and mathematical modeling to produce research such as "Mathematical Modeling of Rumors and Information Propagation in Society." While these articles claim to be defensive, their application in offensive operations is assumed.

Such operations are synchronized by a growing cadre of political technologists. These are leaders, both inside and outside the government, that understand the interrelated nature of the human, political, military, and technological domains. Leveraging this "multi-domain" understanding, they develop and coordinate shaping operations that leverage the cyber and technological domains to affect the social, political, and military domains. As an example,

Alexander Malkevich, a Moscow-based technologist, established the Moscow-based www.USAreally.com website in advance of the 2018 midterm elections in the United States.[12] His mission was to both spread a twisted narrative as well as agitate in a manner aimed at promoting discord among the American populace that was to be picked up by mainstream American news, or at least mainstream news aggregators. The translated personal *description* from his Twitter account states, "Journalist. Media man. A person who is interested in life. And he is not afraid to work in the regions of Russia. And in the name of Russia."[13] This is a political technologist.

Change in the Strategic Center of Gravity

The twentieth century dawned with the most symmetric and kinetic wars in the history of warfare, while the twenty-first century, springboarding off decades of Cold War competition, has dawned with numerous asymmetric and nonkinetic conflicts. During World War I, nations sacrificed hundreds of thousands of lives for mere yards of physical terrain. Today, many actors develop complex designs to slowly gain "yards" in the human domain with ramifications for the physical domain.

Alexander Malkevich, 3 March 2012. (Photo by A. Khmeleva via Wikimedia Commons)

Geography still matters today. The United States' two greatest security measures are still called the Pacific and Atlantic Oceans.[14] Crimea was annexed by Russia largely because of the strategic importance of its Black Sea Port (as well as energy implications).[15] Afghanistan

strategic importance of its Black Sea Fleet (as well as energy implications). Afghanistan instability will persist partly because of its geography.[16] Geography does and always will matter. However, numerous factors, to include technology, have arguably shifted the pendulum toward the human dimension.

This shift toward the human domain was hotly debated inside the U.S. military during the War on Terrorism. After years of debate, the majority seemed to agree with the quote from a 2009 article in Small Wars Journal: "One of the most profound changes the U.S. military must make to be effective at countering insurgency is to shift strategic centers of gravity from the physical to the human aspects of warfare."[17] While generally accepted in counterinsurgency environments, it remains to be seen how this shift toward the human domain will change large-scale combat operations.

This view of the population as the center of gravity took on new meaning in the aftermath of the Arab Spring, as decentralized population movements, enabled by technology, organized and overthrew multiple established autocratic regimes. These actions shocked the world and have been studied by leaders in both the East and the West. These events underscored the power of the human dimension as well as the power of social media to mobilize the masses. Multiple articles in military journals have documented these movements, with a specific focus on the social media that enabled them. Even Gerasimov's 2013 article in Russia's *Military-Industrial Courier*, studied across the West as the genesis of *hybrid* or *gray* warfare, is more a personal reflection of the Arab Spring (as well as the conflicts in Iraq, Afghanistan, and Yugoslavia), than an attempt to create a new type of warfare.[18]

Multiple other state and nonstate actors observed these changes and began exploring the idea of manipulating these movements through cyberspace. Many of these states and actors already have experience manipulating their own populace or organization through information operations, and now seek to extend that experience to other populations and societies.[19] Directly targeting the fabric of society, the true center of gravity of a nation, has massive ramifications for the tactical through strategic levels of war, and is the genesis of this emerging domain of social cybersecurity.

Enabling Changes

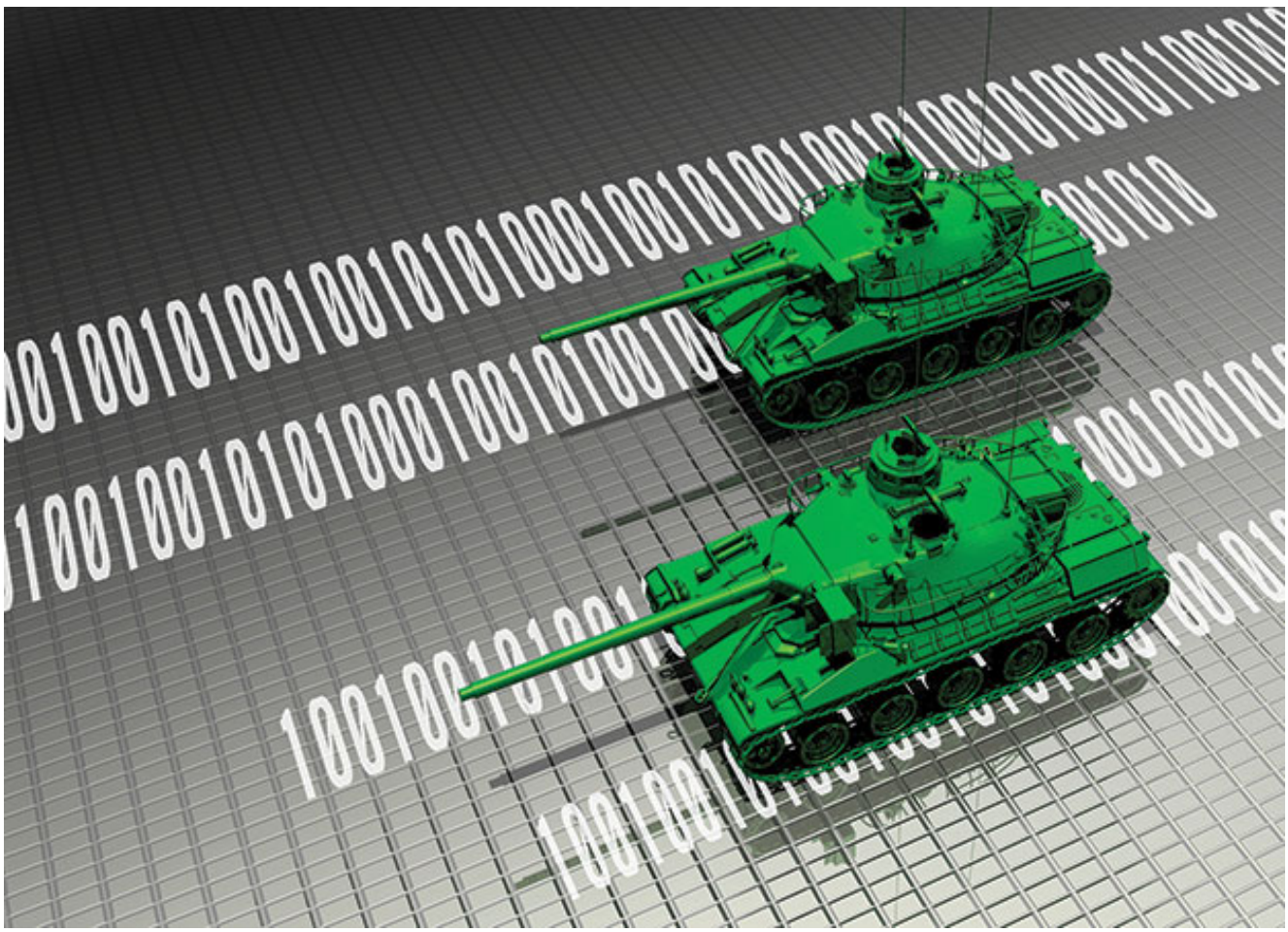
Two changes in human communication and societal information flows have enabled the social cyberthreat. First, technology has waived the requirement for physical proximity to influence society; and, the decentralization of information flows has reduced the cost of entry. Fabio Rugge of the Italian Institute for International Political Studies sums this up with this statement: "Cyberspace is a powerful multiplier of the destabilizing effects of manipulated information because it allows high connectivity, low latency, low cost of entry, multiple distribution points without intermediaries, and a total disregard for physical distance or national borders. Most importantly, anonymity and the lack of certain attribution of an attack make cyberspace the domain of ambiguity."[20]

Decentralization. Over the last thirty years, we have watched as information flows rapidly

decentralized. Historically governments, large organizations, and a few large news outlets controlled most of the formal print, broadcast, and televised news coverage. These organizations controlled the flow of information and generally distributed it uniformly across a society. With the rise of blogs, microblogs, and social networks, most of the world now obtain their information in a nonuniform way on social media.[21] There is now a low cost of entry, financial incentive to create viral content, and anonymity is relatively easy to accomplish. This decentralization has facilitated the entry of external actors with minimal attribution.

Quality control of information flow is now decentralized. Fact checking is now conducted at the user level rather than the journalist level. Users, many who grew up in an era where news was largely trusted, are now unprepared to digest news in an era where truth and untruth are mixed, especially if distortions of the truth are designed to validate their own biases.

The traditional journalism business model requires truth. Journalists lose their jobs, and news organizations lose business if they are consistently in error. The social media business model, largely focused on overall traffic and advertising, does not rely as much on fact checking. However, this is slowly changing, as was observed in the August 2018 stock decline for both Twitter and Facebook, largely attributed to their slow growth while they purge their platforms of accounts that propagate fake news.



(Graphic by victorhabbick via Adobe Stock)

While recent legislation across the world is trying to find a way to centralize control, in all

While recent legislation across the world is trying to find a way to centralize control, in all cases this involves some type of censorship and reduced freedom of speech. In some cases, it could end up in absolute chaos, especially if social media companies are required to provide a platform functionality for people to flag fake or malicious information. If this type of functionality is exposed to users either through an application programming interface (API) or a web/mobile interface, then the same bots that post fake news can now flag all kinds of accurate content as fake at the speed of algorithms, causing exponentially greater damage.

Physical presence not required. For most of history, influence required physical presence or at least physical proximity. To influence the conversation of the Roman forum, the heartbeat of Roman society, an actor or proxy had to be physically present in the forum or at least in Rome, clearly identifiable, and active in the conversation. “Cloak and dagger” operations occurred, but even these operations required physical presence. This requirement held true through the first part of the twentieth century, at which time radio and leaflet operations emerged, not requiring direct physical presence but nevertheless requiring some level of close proximity. Even robust Soviet-era propaganda operations were largely restricted to Eastern Europe and Asia due to geographical limitations. The internet has erased this requirement, with most societies interacting in free and open online environments that allow actors to participate from the far corners of the globe with few national borders in the cyber domain.

Those nations that value freedom of speech and open marketplaces for opinions and ideas are more vulnerable to these threats.[22] This is most evident by the fact that North Korea, arguably the most closed nation on earth, is still largely immune to social manipulation through the internet. Directly influencing the North Korean society still requires physical presence or proximity.

The vulnerability of open societies to social manipulation through technology is exacerbated by the fact that most of these strategic information efforts are launched on global social media platforms that are privately owned and outside of the direct supervision of governments (though influenced by regulation). While all social media companies censor content on their platform, their motivation is generally focused on improving the user experience for the greatest number of people across the world, not national security concerns of any single nation. Choosing sides on any issue is generally bad for business because it alienates a segment of their customer base. Government censorship of content is assumed to be partisan and violates the freedom of speech espoused by these governments. Third-party efforts to censor content have been initiated but to date, these have been narrowly focused and easily circumvented. An example of third-party efforts is the “Social Science One” initiative, a creative partnership between academic researchers, private industry, and funding from across the political spectrum that facilitates third-party research on social media data while maintaining individual privacy. Efforts like this are still in their infancy.

Forms of Social-Cyber Maneuver

As in the physical domain and the traditional cyber domain, the social-cyber domain offers

multiple "forms of maneuver." In this domain, an adversary can manipulate both the *information* as well as the *network*. These networks can be social networks (Sarah and Peter are *friends*), conversation networks (Sarah *replies* to Peter), or informational networks (Sarah and Peter both share the hashtag #NATO).

BEND forms of maneuver. The desired end state for information operations varies. Traditional information operations increase support for the desired narrative and reduce support for the counternarrative. Other operations simply have a desired end state of increased agitation and reduced trust, regardless of the narrative. This agitation serves to drive wedges into a society. Either desired end state are supported by the "BEND" forms of maneuver (as seen in the table).[23]

Table. The BEND Model of Describing Social Cybersecurity Forms of Maneuver (Table by authors) Enlarge the table

	Information Maneuver		Network Maneuver	
	Knowledge network manipulation		Social network manipulation	
	Things you can do by affecting what is being discussed		Things you can do by affecting who is talking/listening to whom	
Positive	**Engage**	Discussion that brings up a related but relevant topic	**Back**	Actions that increase the importance of the opinion leader
	Explain	Discussion that provides details on or elaborates the topic	**Build**	Actions that create a group or the appearance of a group
	Excite	Discussion that brings joy/happiness/cheer/enthusiasm to group	**Bridge**	Actions that build a connection between two or more groups
	Enhance	Discussion that encourages the group to continue with the topic	**Boost**	Actions that grow the size of the group or make it appear that it has grown
Negative	**Dismiss**	Discussion about why the topic is not important	**Neutralize**	Actions that limit the effectiveness of opinion leader such as by reducing the number who can or do follow or reply or attend to
	Distort	Discussion that alters the main message of the topic	**Nuke**	Actions that lead to a group being dismantled
	Dismay	Discussion about a topic that will bring worry/sadness/anger to group	**Narrow**	Actions that lead to the group becoming sequestered from other groups
	Distract	Discussion about a totally different topic and irrelevant	**Neglect**	Actions that reduce the size of the group or make it appear that the group has grown smaller

The BEND forms of maneuver describe how an actor can manipulate the marketplace of beliefs, ideas, and information. These forms of maneuver build on the dismiss, distort, dismay, and distract operations (Press Enter) duced by Ben Nimmo at the Atlantic Councils Digital Forensic

Skip to main content

Research Lab.[24] The BEND model categorizes forms of maneuver by polarity as well as whether the target is the *information* or the *network*.

Information maneuver. Information maneuver is the manipulation of information and the flow or relevance of information in cyberspace. Examples of information maneuver include:

- Misdirection. Introducing unrelated divisive topics into a thread in order to shift the conversation.
- Hashtag latching. Tying content and narratives to unrelated trending topics and hashtags.
- Smoke screening. Spreading content (both semantically and geographically) that masks other operations.
- Thread jacking. Aggressively disrupting or co-opting a productive online conversation.

Network maneuver. Network maneuver is the manipulation of the actual network. In these maneuvers, an adversary maps a social network (once again realizing that an online social network is the projection of social and conversational links in the cyber dimension). Examples of network maneuver include the following:

- Opinion leader co-opting. Gaining access and acknowledgment from an online opinion leader and leveraging his or her influence to spread narrative.
- Community building. Building a community around a topic, idea, or hobby and then injecting a narrative into this group. This was accomplished in Ukraine by building communities of young men around adult content-sharing accounts, and then injecting anti-Ukrainian and pro-Russian rhetoric into these networks.
- Community bridging. Injecting ideas of one group into another. In this case, the adversary will identify two communities, A and B. The adversary would like to inject ideas of group B into group A. This is done by first infiltrating group A, then slowly adding retweets or sharing ideas from group B, bringing the ideas of group B into group A.
- False generalized other. Promoting the false notion that a given idea represents the consensus of the masses and therefore should be an accepted idea or belief by all.

Bots as Force Multipliers

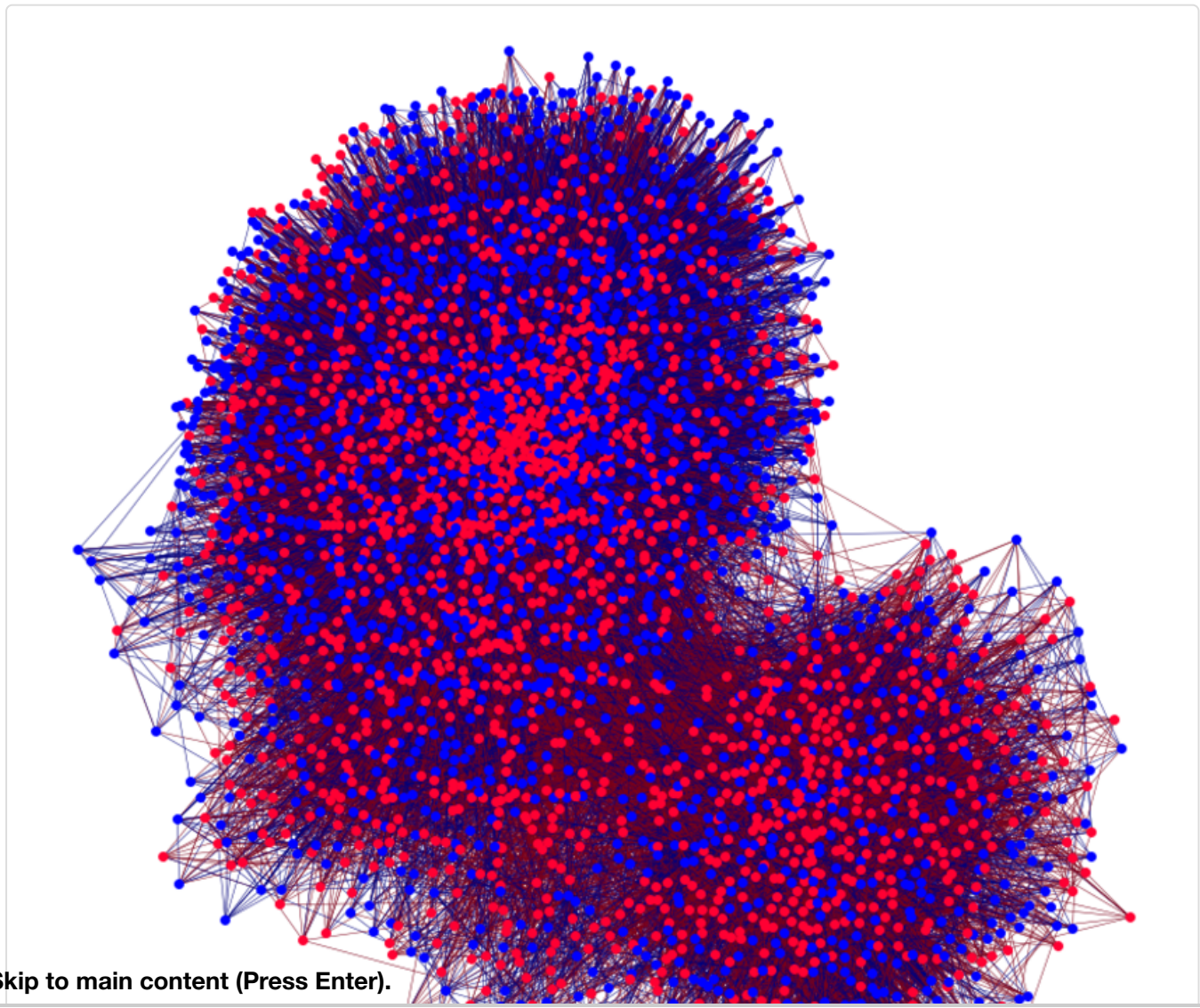
Within the context of information operations, *bots* are increasingly used as force multipliers. They leverage machine learning and artificial intelligence to conduct targeted and timely information transactions at scale while leaving critical nuanced dialogue to human operators. In this context, these human actors are often referred to as “trolls,” which simply differentiates human actors sowing discord from computer actors sowing discord (i.e., “bots”).

A bot is defined as a social media account that uses a computer to automate social media tasks. For example, in the Twitter environment, a bot account can automatically tweet, retweet, follow, friend, reply, quote, and like. The bot creator can use creative means to generate content, either “scraping” (and automatically summarizing) from elsewhere on the

web, retweeting existing content, manipulating existing content from other human users, or creating their own content through a combination of human input and artificial intelligence. Having created content, the bot creator can manipulate tweet timing to appear human (or if appearing human is not critical to the operation, can conduct thousands of actions around the clock). Finally, these bots are often deployed in bot nets (sometimes called bot “armies” or “coordinating” bots) where they friend, follow, and otherwise promote each other to appear popular.

Bots are used for a wide variety of reasons, creating effects that are positive, nuisance, or malicious. Some examples of positive bots include personal assistants and accounts that notify the public of natural disasters. Nuisance bots distribute spam with content ranging from commercial advertising to adult content. Malicious bots are typically involved in propaganda, suppression of dissent, intimidation, and network infiltration/manipulation.[25]

Although we often attempt to classify an account as bot or human, there is often a spectrum of automated involvement with an account. Many accounts are not strictly automated (all transactions executed by a computer). These accounts have human intervention to contribute nuanced dialogue while a computer executes tasks at scale in the background. When combined with artificial intelligence, these bots conduct sophisticated operations at scale at the speed of algorithms (see figure).



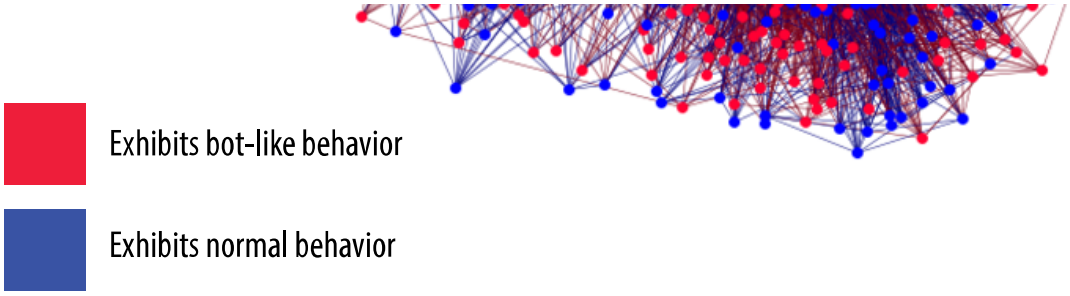


Figure. Bot Involvement in the Core Twitter Political Conversation Surrounding Recent Election in Sweden
(Figure by authors)

Enlarge the figure

Conclusion

A new-generation war will be dominated by information and psychological warfare that will seek to achieve superior control of troops and weapons and to depress opponents armed forces personnel and population morally and psychologically. In the ongoing revolution in information technologies, information and psychological warfare will largely lay the groundwork for victory.

—Russian *Military Thought*, 2013[26]

Arguably, the greatest strategic weakness for any country is internal, not external. Leaders must understand social cybersecurity in order to defend these internal weaknesses from external manipulation. We as military leaders must understand that one of the information blitzkrieg lines of effort will be to drive a wedge of distrust between us and the society we defend as well as civil leadership that leads us. An untrusted institution will be underfunded, underused, and underperforming.

If one of our primary missions is to "sustain American influence abroad," then we need to find our role in promoting American values in this international marketplace of beliefs and ideas within a coordinated interagency effort. This influence will range from online interaction to the handshake from a forward-deployed platoon leader.

Military leaders must enact policies that enable freedom of maneuver in the relevant information environments. A recent RAND information operations report concluded that the DOD must change its policy in order to fully enable ethical maneuver within the information domain.[27] Most social cybersecurity practitioners (both bot creators and bot defenders) use APIs and open source technology to access and maneuver in this data environment. In other words, APIs are the access point for both offensive and defensive social cyber operations. In the military, policies and authorities to access APIs are severely restricted for some organizations while not well-defined for others. We need agile policies that enable initiative in a dynamic information environment while protecting the privacy of well-intentioned individuals and remaining within the authorities granted to the DOD.

Skip to main content (Press Enter).

In summary, we must directly educate our force and indirectly educate our society about the

decentralized nature of the modern information environment, the risks that exist, and ways and means to individually vet the facts and opinions that we digest and allow to shape our beliefs and attitudes. We must develop a multidisciplinary approach to social cybersecurity. We must build relevant policy that enables social cybersecurity. We must seek to remove any wedge of distrust artificially driven between our military and the society we defend. We must search for the DOD role in an interagency effort to combat the information blitzkrieg we face today. Social cybersecurity is a required discipline for the foreseeable future.

This work was supported in part by the Office of Naval Research (ONR) Multidisciplinary University Research Initiative Award N000141812108, Office of Naval Research Minerva Awards N00014-13-1-0835/N00014-16-1-2324, and the Center for Computational Analysis of Social and Organization Systems (CASOS). The views and conclusions contained in this article are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the ONR or the U.S. government.

Notes

1. Kathleen M. Carley et al., "Social Cyber-Security," in *Social, Cultural, and Behavioral Modeling: 11th International Conference, SBP-BRiMS 2018, Washington, DC, USA, July 10–13, 2018, Proceedings*, ed. Halil Bisgin et al. (New York: Springer, 2018), 389–94.
2. Joshua Yaffa, "Dmitry Kiselev Is Redefining the Art of Russian Propaganda," *The New Republic* (website), 1 July 2014, accessed 14 November 2018, **https://newrepublic.com/article/118438/dmitrykiselev-putins-favorite-tv-host-russias-top-propogandist (https://newrepublic.com/article/118438/dmitrykiselev-putins-favorite-tv-host-russias-top-propogandist)**.
3. Stephen Townsend, "Accelerating Multi-Domain Operations: Evolution of an Idea," Modern War Institute at West Point, 23 July 2018, accessed 14 November 2018, **https://mwi.usma.edu/accelerating-multi-domain-operations-evolution-idea/ (https://mwi.usma.edu/accelerating-multi-domain-operations-evolution-idea/)**; Valery Gerasimov, "The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations," *Military Review* 96, no. 1 (January-February 2016): 23–29.
4. Carley et al., "Social Cyber-Security."
5. "Legacy Homepage," U.S. Department of Defense, accessed 16 November 2018, **https://dod.defense.gov/ (https://dod.defense.gov/)**.
6. Peter Pomerantsev, "Russia and the Menace of Unreality: How Vladimir Putin is Revolutionizing Information Warfare," *The Atlantic* (website), 9 September 2014, accessed 14 November 2018, **https://www.theatlantic.com/international/archive/2014/09/russia-putin-revolutionizing-information-warfare/379880/ (https://www.theatlantic.com/international/archive/2014/09/russia-putin-revolutionizing-information-warfare/379880/)**.
7. Gerasimov, "The Value of Science is in the Foresight."
8. Charles K. Bartles, "Getting Gerasimov Right," *Military Review* 96, no. 1 (January-February 2016): 30–38.
9. Ibid.
10. Steve Abrams, "Beyond Propaganda: Soviet Active Measures in Putin's Russia," *Connections: The Quarterly Journal* 15, no. 1 (2016): 5–31.
11. Harold D Lasswell, "The Strategy of Soviet Propaganda," *Proceedings of the Academy of Political Science* 24, no. 2 (1951): 66–78.
12. Tim Johnson, "Exclusive: 'Little Russian Media Project' Tries to Turn America against Itself," McClatchy, last updated 10 June 2018, accessed 21 December 2018, **https://www.mcclatchydc.com/news/nation-**

world/national/national-security/article213403299.html (https://www.mcclatchydc.com/news/nation-world/national/national-security/article213403299.html).
13. Alexander Malkevich (@McCevich), "Journalist. Media man. A person who is interested in life. And he is not afraid to work in the regions of Russia. And in the name of Russia [in Russian]," Twitter, accessed 21 December 2018, **https://twitter.com/McCevich (https://twitter.com/McCevich)**.
14. Peter Zeihan, *The Accidental Superpower: The Next Generation of American Preeminence and the Coming Global Disorder* (New York: Twelve, 2014).
15. John Biersack and Shannon O'Lear, "The Geopolitics of Russia's Annexation of Crimea: Narratives, Identity, Silences, and Energy," *Eurasian Geography and Economics* 55, no. 3 (2014): 247–69.
16. Robert D. Kaplan, "The Revenge of Geography," *Foreign Policy*, no. 172 (2009): 96–105.
17. James A. Gavrilis, "A Model for Population-Centered Warfare: A Conceptual Framework for Analyzing and Understanding the Theory and Practice of Insurgency and Counterinsurgency," Small Wars Journal, 10 May 2009, accessed 14 November 2018, **http://smallwarsjournal.com/blog/journal/docs-temp/241-gavrilis.pdf (http://smallwarsjournal.com/blog/journal/docs-temp/241-gavrilis.pdf)**.
18. Bartles, "Getting Gerasimov Right."
19. Lasswell, "The Strategy of Soviet Propaganda."
20. Fabio Rugge, "'Mind Hacking': Information Warfare in the Cyber Age," Analysis No. 319, Italian Institute for International Political Studies, 11 January 2018, accessed 14 November 2018, **https://www.ispionline.it/en/pubblicazione/mind-hacking-information-warfare-cyber-age-19414 (https://www.ispionline.it/en/pubblicazione/mind-hacking-information-warfare-cyber-age-19414)**.
21. Elisa Shearer and Jeffrey Gottfried, "News Use Across Social Media Platforms 2017," Pew Research Center, 7 September 2017, accessed 14 November 2018, **http://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/ (http://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/)**.
22. Robert F. Baumann, "A Central Asian Perspective on Russian Soft Power: The View from Tashkent," *Military Review* 98, no. 4 (July-August 2018): 50–63.
23. The "BEND" acronym is derived from the sixteen forms of maneuver presented in the table: four start with "B," four with "E," four with "N," and four with "D."
24. Ben Nimmo, "Anatomy of an Info-War: How Russia's Propaganda Machine Works, and How to Counter It," *Central European Policy Institute* 15 (2015).
25. Cristian Lumezanu, Nick Feamster, and Hans Klein, "#bias: Measuring the Tweeting Behavior of Propagandists," *Proceedings of the Sixth International Conference on Weblogs and Social Media* (Palo Alto, CA: The AAAI Press, 2012), 210–17; John-Paul Verkamp and Minaxi Gupta, "Five Incidents, One Theme: Twitter Spam as a Weapon to Drown Voices of Protest" (paper presentation, 3rd USENIX Workshop on Free and Open Communication on the Internet, Washington, DC, 13 August 2013), 1–7; Rosie Alfatlawi, "Thousands of Twitter Bots Are Attempting to Silence Reporting on Yemen," Al Bawaba: The Loop, 22 November 2017, accessed 16 November 2018, **https://www.albawaba.com/loop/original-saudi-bots-yemen-suffering-1051564 (https://www.albawaba.com/loop/original-saudi-bots-yemen-suffering-1051564)**; Matthew Benigni and Kathleen M. Carley, "From Tweets to Intelligence: Understanding the Islamic Jihad Supporting Community on Twitter," in *Social, Cultural, and Behavioral Modeling: 9th International Conference, SBP-BRiMS 2016, Washington, DC, USA, June 28–July 1, 2016, Proceedings*, ed. Kevin S. Xu et al. (New York: Springer, 2016), 346–55.
26. Sergey G. Chekinov and Sergey A. Bogdanov, "The Nature and Content of a NewGeneration War," *Military Thought* 4 (2013): 12–23.
27. William Marcellino et al., "Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations" (Santa Monica, CA: RAND Corporation, 2017).

Lt. Col. David Beskow, U.S. Army, is a PhD candidate in the School of Computer Science at Carnegie Mellon University. He holds a BS from the United States Military Academy in civil engineering and an MS from the Naval Postgraduate School in operations research. During his career, Beskow served as an infantry leader in the 82nd Airborne Division and the 4th Infantry Division. As an FA49 operations research and systems analyst (ORSA), Beskow served as an assistant professor at

West Point and as an ORSA analyst at the U.S. Army Intelligence and Security Command. Beskow's current research develops machine learning algorithms to detect and characterize online bots and the disinformation campaigns they inhabit.

Kathleen M. Carley, PhD, is a professor of societal computing in the School of Computer Science at Carnegie Mellon University, an IEEE Fellow, the director of the Center for Computational Analysis of Social and Organizational Systems (CASOS), and the CEO of Netanomics. She is the 2011 winner of the Simmel Award from the International Network for Social Network Analysis and the 2018 winner of the National Geospatial-Intelligence Agency Academic Award from GEOINT.

March-April 2019

Back to Top

Skip to main content (Press Enter).

QUICK LINKS

About Military Review (MR) (/Journals/Military-Review/About-Military-Review/)

Subscribe to MR (/Journals/Military-Review/Subscribe-to-Military-Review)

DePuy Writing Competition (/Journals/Military-Review/DePuy-Writing-Competition)

Current Edition (/Journals/Military-Review/English-Edition-Archives/July-August-2021/)

MR English Archives (/Journals/Military-Review/English-Edition-Archives/)

Online Exclusive Article Archive (/Journals/Military-Review/English-Edition-Archives/#online-exclusives)

Plagiarism Policy (/Portals/7/army-university-press-plagiarism-policy.pdf)

Featured Book Reviews (/Journals/Military-Review/MR-Book-Reviews/)

Book Review Archives (/Journals/Military-Review/MR-Book-Reviews/Book-Review-Archives/)

Directors Select Articles (/Journals/Military-Review/Directors-Select-Articles/)

Document Word Search (/Journals/Military-Review/MR-Tut/MR-Search-Tut/)

MR Submission Guidelines (/Journals/Military-Review/MR-Article-Submission-Guide/)

Contact MR (/About/Contact/#mr-contact)

Book Review Submission Guide (/Journals/Military-Review/MR-Book-Review-Submission-Guide/)

War Poetry Submission Guide (/Journals/Military-Review/MR-War-Poetry-Submission-Guide/)

Home (/)

Publish With Us (/Publish-With-Us/)

NCO Journal Submission Guide (/Journals/NCO-Journal/NCO-Journal-Submission-Guidelines/)

Military Review Submission Guide (/Journals/Military-Review/MR-Article-Submission-Guide/)

Skip to main content (Press Enter).

Monographs and Books Submission Guide (/Books/Books-and-Manuscript-Guide/)

Journal of Military Learning Submission Guide (/Journals/Journal-of-Military-Learning/Author-Submission-Guidelines/)

Plagiarism Policy (/Portals/7/army-university-press-plagiarism-policy.pdf)

Special Topics (/Special-Topics/)

New Extended Battlefield (/Online-Publications/New-Extended-Battlefield/)

Primer on Urban Operations (/Online-Publications/Primer-on-Urban-Operations/)

Future Warfare Writing Program (/Special-Topics/Future-Warfare-Writing-Program/)

Future Warfare Writing Program Submission Guidelines (/Special-Topics/Future-Warfare-Writing-Program/Future-Warfare-Writing-Program-Submission-Guidelines/)

Books (/Books/)

Browse Books (/Books/Browse-Books/)

Large-Scale Combat Operations Book Set (/Books/Large-Scale-Combat-Operations-Book-Set/)

Order a Book (mailto:usarmy.leavenworth.tradoc.mbx.armyu-aup-rp@mail.mil?Subject=Army%20Press%20Book%20Request&Body=Dear%20Research%20and%20Books%20Team%2C%0A%0AI%20would%20like%20to%20request%20a%20copy%20of%20the%20following%20book%3A%0A%0A%0A%0A%0A%5BHard%20copies%20of%20publications%20are%20becoming%20very%20limited%20in%20number.%20%20Our%20current%20budget%20severely%20limits%20the%20number%20printed%20of%20new%20publications.%20Existing%20stocks%20are%20becoming%20quickly%20depleted.%20%20We%20will%20attempt%20to%20fill%20requests%20as%20stocks%20last%2C%20many%20of%20our%20most%20popular%20titles%20are%20out%20of%20print.%20The%20digital/pdf%20files%20are%20formatted%20for%20easy%20printing%20and%20optimum%20viewing%20on%20most%20devices.%5D%0A)

Staff Ride Handbooks (/Books/CSI-Press-Publications/Staff-Ride-Handbooks/#staff-rides)

Journals

NCO Journal (/Journals/NCO-Journal/)

Military Review (/Journals/Military-Review/)

Edición Hispanoamericana (/Journals/Edicion-Hispanoamericana/)

Skip to main content (Press Enter).

Edição Brasileira (/Journals/Military-Review/Edicao-Brasileira/)

Edição Brasileira (/Journals/Military-Review/Edicao-Brasileira/)

Journal of Military Learning (/Journals/Journal-of-Military-Learning/)

Educational Services

Documentaries (/Educational-Services/Documentaries/)

Staff Ride Team (/Educational-Services/Staff-Ride-Team-Offerings/)

Military History Instruction Support Team (/Educational-Services/Military-History-Instruction-Support-Team/)

Frontier Army Museum (/Educational-Services/Frontier-Army-Museum/)

Army University Press Social Media

Facebook (https://www.facebook.com/ArmyUniversityPress/) | **Twitter (https://twitter.com/ArmyUPress)** | **LinkedIn (https://www.linkedin.com/company/armyuniversitypress/)** | **YouTube (https://www.youtube.com/channel/UCX9G3c6jkROVZ0tXr4gvUKQ/)**

NCO Journal Social Media

Facebook (https://www.facebook.com/NCOJournal/) | **Twitter (https://twitter.com/NCOJournal)** | **Instagram (https://www.instagram.com/ncojournalofficial/)**

Military Review LATAM Social Media

Facebook (https://www.facebook.com/MilitaryReviewLATAM/) | **Twitter (https://twitter.com/MilReview_LATAM)**

Army University Press Offices

290 Stimson Ave. Fort Leavenworth, Kansas 66027 **Contact Us (/About/Contact/)** | 913-684-2127

About Us (/About/)

The US Army's premier multimedia organization that focuses on advancing the ideas and insights military professionals need to lead and succeed.

Legal and Administrative Notices

Privacy and Security Policy (/About/Legal-Administrative/Privacy-and-Security-Policy/)

User Terms of Agreement (/About/Legal-Administrative/User-Terms-of-Agreement/)

Publishing Disclaimer (/About/Legal-Administrative/User-Terms-of-Agreement/#publishing-disclaimer)

External Links (/About/Legal-Administrative/User-Terms-of-Agreement/#external-links)

Section 508 (/About/Legal-Administrative/User-Terms-of-Agreement/#section-508)

Copyright Disclaimer (/About/Legal-Administrative/User-Terms-of-Agreement/#copyright)

Web Policy (http://dodcio.defense.gov/DoD-Web-Policy/)

Army University (https://www.armyuniversity.edu/)

ArmyU Overview Booklet (/Portals/7/home/the-army-university-overview-booklet.pdf)

ArmyU Overview Placemat (/Portals/7/home/the-army-university-placemat.pdf)

Information Quality (https://www.defense.gov//Resources/DOD-Information-Quality-Guidelines/)

Plain Writing Act (http://www.esd.whs.mil/DD/plainlanguage/)

Privacy Program (https://dpcld.defense.gov/Privacy.aspx)

No FEAR Act (https://www.army.mil/article/236698)

FOIA (https://www.rmda.army.mil/foia/RMDA-FOIA-Division.html)

Open GOV (http://open.defense.gov/)

Strategic Plan (https://cmo.defense.gov/Publications/NDBOP.aspx)

USA.gov (https://www.usa.gov/)