National Intelligence University

Spring Quarter 2023

MST 680
Strategic Intelligence and Information Power
Professor R. C. Rochte

Midterm – Short Essay

Submitted by

Alejandro F. Sosa

I verify that this submission is my own original work.

25 April 2023

The modern era has been referred to as the information age. It is a period in time in which information or data has never been more accessible to the global population. However, this dramatic increase in access to information has also exposed vulnerabilities in open societies. There are multiple different philosophies competing for primacy in the world order. The United States once considered itself to be the "city upon the hill" built for life, liberty, and the pursuit of happiness, a nation that welcomed the tired, poor, and huddled masses. The United States now faces multiple competing messages. Islamic extremists have posited that the United States represents a nation meant to tempt devout Muslims to stray from the path of God. China seeks to become a global hegemon and acknowledges that it must gain strength while marginalizing the United States in order to achieve this goal. China has thus sought to compete with the United States and become a preferred global ally, offering the global south an alternative to a Western-led world order.[1] Russia has sought to increase its global position by both retaking territories lost during the dissolution of the Soviet Union and working to degrade the modern global institutions and nations that currently bind the current world order. Russia has worked to undermine basic United States traditions and norms by meddling in the 2016 elections, amplifying voices that sow dissent and discord in society, and increasing the stature of politicians that are increasingly nationalistic and isolationist in order to degrade NATO and other global institutions that it believes pose a threat to Russian security[2]. The relative position and security of the United States are at stake in this war of ideas, and the increasing integration of information technology across everyday life has created new vulnerabilities by allowing foreign adversaries to push their messages directly to individual citizens via social media and through the global

[1] Hal Brands Beckley Michael, "What Does China Want?," *Foreign Policy*, August 13, 2022, accessed April 25, 2023, https://foreignpolicy.com/2022/08/13/what-china-wants-us-conflict/.
[2] "Russia as a Hurricane, China as Climate Change: Different Ways of Information Warfare," *War on the Rocks*, last modified January 21, 2020, accessed July 10, 2020, https://warontherocks.com/2020/01/russia-as-a-hurricane-china-as-climate-change-different-ways-of-information-warfare/.

media ecosystem. Russia and China have been able to effectively wield information via both public sector messaging, the launch of successful private corporations, and cyber-attacks in order to achieve their political goals[3].

In order to understand how international actors are manipulating the information environment, or the "aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.[4]" It is important to understand all of the different components that comprise the information environment. *The Joint Concept for the Operations in the Information Environment* lays out three aspects to understand when evaluating the information: human, physical, and informational. The human aspects are all of the things that suggest how a human might behave under particular circumstances. These aspects could relate to their culture, where they place value, nuances in language, historical, and physical or psychological considerations. For example, there are many people who lived through the great depression who chafe at the idea of wasting food despite its relative cheapness and high availability today. The physical aspects of information power relate primarily to the geography that impacts a given actor, including things like territorial boundaries and natural and manufactured terrain, such as deserts, dams, or bodies of water. Finally, informational aspects of the information environment reflect how data is communicated and exchanged, such as telecommunications, in-person meetings, or global media.[5] It is this last aspect of the information environment that is often used to exert information power. However, it is critical to understand all of the aspects of the information environment in order to achieve the desired effect.

---

[3] Timothy D Haugh, Nicholas J Hall, and Eugene H Fan, "16th Air Force and Convergence for the Information War" (n.d.).
[4]Joint Chiefs of Staff, Joint Concept for Operating in the Information Environment (JCOIE), 25 July 2018.
[5] Ibid

China and Russia have both been conducting information operations on the United States and the international community. It is imperative to understand how they influence the information environment in order to defend against it. There is a clear intersection between military, governmental, and civilian information capabilities, which pose significant challenges to the United States in attempts to stem the national information power of its adversaries both due to the division between national defense and law enforcement as well as the legal protection for freedom of speech which make it possible for foreign messaging campaigns to be amplified domestically. Russia and China regularly wield information power via cyberspace[6]. They leverage the internet, social media, and traditional media to ensure the greatest visibility of their desired message. For example, although it is now public knowledge that the Chinese application TikTok has been stealing user data and sending data beyond what is inherent in the application also resident on the device back to Beijing because it is a private corporation being used by United States citizens, there must be a political solution rather than an Intelligence Community or Military Solution.[7] Traditionally, these institutions have avoided the political fray as a means of ensuring continued public trust.

Due to the constraints that the United States Constitution, legal code, and traditions place on the role of the military, the United States military's concept of Information Warfare is inherently limited to the areas in which they can make an impact. Unfortunately, there is no grand unified strategy for the United States to achieve success in the Information Environment, which coordinates and synchronizes all of the different entities active in the Information Environment. There is no office that hones the message of the United States as an idea and

[6] "Russia as a Hurricane, China as Climate Change."
[7] Bryce Johnston, "Information Operations in the Era of TikTok: Some Thoughts for My Fellow Junior Leaders," *Modern War Institute*, last modified February 9, 2021, accessed April 25, 2023, https://mwi.usma.edu/information-operations-in-the-era-of-tiktok-some-thoughts-for-my-fellow-junior-leaders/.

coordinates it with the Department of State, Department of Defense, Hollywood, Silicon Valley, and with allies. Even then, the Department of Defense's approach to information operations has changed and evolved constantly over the past decade. This could be due to a failure to understand the information environment. It could also be due to the rapidly changing and evolving nature of information technology. Russia and China have been effectively creating and disseminating propaganda for decades now. Rather than merely targeting their own populations, they are exporting these messages. Instead of focusing on messaging and content, United States information operations tend to be limited to informational aspects of the information environment, which focus on the technical defense of United States critical infrastructure as well as defending against malicious actors by preventing network intrusion, data exfiltration, or defending forward by shutting down malicious farms of bots which can be used to amplify misinformation. An example of how the United States military has proposed to engage in information is the Air Force developed the concept of convergence, which is the integration of cyber operations, electronic warfare, intelligence surveillance and reconnaissance, military information support operations, and military deception in order to create impacts greater than any individual function could create individually.

A cornerstone of modern society, which is often underappreciated by the general public until something goes wrong, is the role that infrastructure plays in daily life. The United States Department of Homeland Security identified 16 areas of critical infrastructure, such as the financial services, energy, transportation, water, and information technology sectors, among others. The vast majority of infrastructure sectors also rely upon the energy and information technology sectors, so an attack on either one of these areas would create cascading problems across multiple other sectors. The increasing utilization of Supervisory Control and Data

Acquisition systems, or computer-based control systems in the energy sector, means that by conducting a cyber-attack on energy systems or across national information technology, a foreign adversary could cripple the United States without ever firing a shot. In May of 2021, the Colonial Pipeline was shut down due to a ransomware attack that targeted its billing software. The pipeline supplies about 45% of all of the fuel utilized on the East Coast. Within four days, 71% of filling stations in Charlotte, NC, had run out of gasoline, and by the seventh day, 87% of gas stations ran out of fuel in Washington, DC. Public behavior changed overnight as people rushed out to ensure they had a full tank of gas, and many people worked from home during that time frame.

The problem of cybersecurity, however, is not solely a problem of the energy sector. The composition of the United States public infrastructure has become increasingly fragile.[8] Many utility companies, including power generation, water supply and treatment, transportation, and even emergency services, have become increasingly privatized. As ownership has shifted from the government to private control, so have operational incentives. Governments seek to provide effective and efficient service to its population. Often, this requires having redundant capabilities, continuity of operations plans, and the assurance that the public good is always a primary factor. Private industry, on the other hand, does not serve the public; it serves shareholders with the sole goal of increasing value. Additionally, utilities that have privatized often push for increased deregulation as a means of increasing profit. The chase for profit has also led to many mergers in the utility industry, meaning that economies of scale reduce costs and increase profits. These three trends of mergers, deregulation, and increasing integration of

[8] Robert A Miller and Irving Lachow, "Strategic Fragility: Infrastructure Protection and National Security in the Information Age" (2008).

information technology while reducing staff have made United States critical infrastructure increasingly vulnerable to failure.

There are a few possible ways to begin to reverse the trend of weakening United States infrastructure. However, they are all likely to be unpopular and challenged by powerful and well-funded opponents. It is also unlikely that any significant changes will be made until after an emergency crisis threatens public faith in the current systems. In order to protect critical infrastructure, the government, either at the federal or local level, could increase regulatory requirements across the different forms of critical infrastructure. However, regulations are only as good as the entity that oversees compliance with regulations. The regional federal reserve chairs were encouraged to be more flexible with regard to overseeing regional banks like Silicon Valley Bank, which meant that the composition of Silicon Valley Banks' holdings was largely overlooked.[9] The crisis could have been preventable if the regulator had done its job effectively. Alternatively, the United States could attempt to stand up an organization whose mission was to provide defense of critical infrastructure, a mission which currently resides with the many different agencies under the Department of Homeland Defense. However, they do not provide cybersecurity across the board. The organizations most capable of this task are the National Security Agency and Cyber Command or the United States Military. However, there are multiple concerns about such a proposal, such as the divisions between state and local government. Would the National Guard or Federal Reserve have to be activated for these elements to conduct these functions, and for how long? How much would this increase the federal operating budget? Finally, does this invite further government intrusion into private operations? Alternatively, the Federal Government could nationalize these industries and return them to the status of providing

[9] Donald Kohn and David Dollar, "Will Silicon Valley Bank's Collapse Lead to a Financial Crisis?," *Brookings*, April 4, 2023, accessed April 25, 2023, https://www.brookings.edu/podcast-episode/will-silicon-valley-banks-collapse-lead-to-a-financial-crisis/.

public services rather than seeking profit, but that would create massive upheaval in the financial markets and generate a massive public outcry. There are few solutions that a politician who aims to continue holding public office could likely implement in any sustainable way.

Finally, among the protections granted in the United States Constitution are the right to freedom of the press and free speech. While these represent the foundations of a free and open society, they can represent a conflict in the context of information power and information warfare. Traditionally, new media, or journalists, sought to inform the public on matters that impacted them, their nation, or their livelihood. The rise of the 24-hour news cycle shifted the goals of media from informing to entertaining or captivating, often at the expense of journalistic integrity. Of course, media does not only impact and shape the conduct of operations. The "CNN effect," or the collective impact of all real-time news coverage, has driven United States involvement in a given international crisis. Attention is a zero-sum game, and what media sources choose to focus on can impact how constituents interpret and react to a given situation. However, previously, there may have existed a single mono-culture in which most news organizations delivered similar content about similar events worldwide. The modern media ecosystem has evolved so that people can tailor their information environment.

There is such a glut of content that has been produced, both for sale and for free, to every type of audience that it has been possible for individuals and groups to define their own information environment. In order to conduct effective information operations, it is imperative to understand the modes of information consumption of the targeted audience. The intelligence community requires deep anthropological knowledge of any population it seeks to influence. The only way to truly wield information power over a given population is to create a closed society in which content is extremely curated, outside information is both inaccessible and criminalized,

and speech is limited to that which furthers the aims of the state. This is part of why China and Russia remain relatively difficult to impact via information operations; they have effectively removed outside influences via their direct control over their citizens. The concept of a single information environment may then be overstated. It has become ever more critical for the Intelligence Community and military to understand the information environments as they exist in a given area. Where do Malians turn for news? Who are the most trusted personalities in the Wuhan province of China? Evaluating the world via Twitter tracking or mentions is planning for failure. In order for the United States to effectively campaign in the information environment, we require a unified strategy that incorporates all aspects of the relative information environment, and we require coordination among the different levers of influence, diplomatic, informational, and military.

Bibliography

Beckley, Hal Brands, Michael. “What Does China Want?” *Foreign Policy*, August 13, 2022. Accessed April 25, 2023. https://foreignpolicy.com/2022/08/13/what-china-wants-us-conflict/.

Dollar, Donald Kohn, and David. “Will Silicon Valley Bank’s Collapse Lead to a Financial Crisis?” *Brookings*, April 4, 2023. Accessed April 25, 2023. https://www.brookings.edu/podcast-episode/will-silicon-valley-banks-collapse-lead-to-a-financial-crisis/.

Haugh, Timothy D, Nicholas J Hall, and Eugene H Fan. “16th Air Force and Convergence for the Information War” (n.d.).

Johnston, Bryce. “Information Operations in the Era of TikTok: Some Thoughts for My Fellow Junior Leaders.” *Modern War Institute*. Last modified February 9, 2021. Accessed April 25, 2023. https://mwi.usma.edu/information-operations-in-the-era-of-tiktok-some-thoughts-for-my-fellow-junior-leaders/.

Klein, Aaron. “No, Dodd-Frank Was Neither Repealed nor Gutted. Here’s What Really Happened.” *Brookings*, May 25, 2018. Accessed April 25, 2023. https://www.brookings.edu/research/no-dodd-frank-was-neither-repealed-nor-gutted-heres-what-really-happened/.

Miller, Robert A, and Irving Lachow. “Strategic Fragility: Infrastructure Protection and National Security in the Information Age” (2008).

“Russia as a Hurricane, China as Climate Change: Different Ways of Information Warfare.” *War on the Rocks*. Last modified January 21, 2020. Accessed July 10, 2020. https://warontherocks.com/2020/01/russia-as-a-hurricane-china-as-climate-change-different-ways-of-information-warfare/.