THE CHANGING NATURE OF WARFARE IN THE TWENTY-FIRST CENTURY

Joseph Hobbs
MS.110: American Military History
Due April 30, 2022

Warfare is as old as humankind itself. Remaining intertwined with human nature, the principles of warfare are an invariant in our society, unweathered by the passage of time, the quickening pace of technological improvement, and the chaos of changing political boundaries. In his book *On War*, the renowned classical war scholar Carl von Clausewitz tells us that warfare is "an act of force to compel our enemy to do our will"[1]. If we are to investigate the changing nature of warfare in the twenty-first century, we must first understand changes in the nature of that defining act of force. And to do that, we look at one of the greatest changes on the international stage in the last 20 years: the advent of the Internet. Between 2002 and today, the number of people connected to the Internet has increased nearly by a factor of ten[2], drastically changing the means through which groups may leverage the elements of national power to wage warfare. Most notably, the two significant changes to this defining act of force are in the increase of psychological operations against civilian targets and the new threat of cyber operations against economic and military-economic structures.

The cost to conduct psychological operations has decreased unlike ever before in human history. The Department of Defense defines psychological operations as the "planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, [and] reasoning"[3]. Psychological operations target a key element of warfare: the civilian population. The civilian population's importance is best explained by Clausewitz's "paradoxical trinity" of war[4]. The trinity of warfare consists of the government, the military, and the people. The people's support gives legitimacy to the government and to its military; without it, neither the government nor the military is capable of operating. Therefore, waging war in the

---

[1] Clausewitz, *On War*, 75.
[2] Roser, Ritchie, and Ortiz-Ospina, "Internet."
[3] Department of the Army, *ATP 3-13.1*, 3-5.
[4] Clausewitz, *On War*, 89.

psychological domain (and specifically the sector of the psychological domain that exists through the Internet) means changing public opinion and undermining support for governmental and military operations. The government (and its military) operates at the leisure of the people; if a nation can convince its enemy's people that their government is corrupt, incapable, or otherwise illegitimate, the government's ability to leverage diplomacy, information, military, and economy will decrease drastically.

We observe that the advent of the Internet functions as a powerful tool through which our adversaries are easily able to increase their capability for psychological operations. And our adversaries show no mercy; many highly active areas of political debate in the United States are fueled on a daily basis by social media "trolls" working at the Internet Research Agency (IRA), a Russian corporation headquartered in St. Petersburg[5]. Through its psychological operations, the IRA attempts to undermine the American trinity of warfare through decreasing popular support and increasing perceived levels of corruption of the U.S. government.

Since its emergence into popular usage, certain corners of the Internet have been ablaze with arguments around personal and collective identity, primarily race, sexuality, and religion. In recent years, many of these arguments have experienced a paradigm shift towards subjects such as the Black Lives Matter movement, immigration policy, the LGBTQ+ community, and the ongoing discussion regarding the future of Second Amendment rights. "The Tactics and Tropes of the Internet Research Agency" by data analysis company New Knowledge, made publicly available by the University of Nebraska at Lincoln, analyzes the IRA's behaviors during the time window leading up to, during, and immediately following the 2016 presidential election. The analysis by New Knowledge revealed that the IRA targeted communities with personal

[5] Thompson and Lapowsky, "Russian Trolls Divide America."

connections to the aforementioned issues to create increased tribalism, especially among U.S. voters.

The IRA's misinformation campaign during the 2016 election was unprecedented in its breadth, depth, and scope, reaching across multiple social media platforms and used both humans and bots to create content. Black Lives Matter and police brutality were far and away the primary subject of the IRA's propaganda efforts. New Knowledge found 1,107 videos on YouTube that were created by confirmed or suspected IRA accounts, of which 1,063 (96%) were focused on Black Lives Matter or police brutality in the United States. New Knowledge also provides a list of 16 domain names, attributing their registration to the IRA during the 2016 election cycle. 10 (63%) of these domain names are connected to the ongoing Black power culture war in the United States. Eight of them contain the keyword "black" and the remaining two are "dntshoot.com" and "donotshoot.us", clearly referring to police brutality in the United States[6].

Instagram activity followed similar trends. Out of the top 10 IRA Instagram accounts (sorted by number of combined likes and comments), three appealed to the Black community ("blackstagram_", "sincerely_black_", and "afrokingdom_"), three appealed to American conservatives and police supporters ("_american.made", "mericanfury", and "pray4police"), one appealed to Christians ("army_of_jesus_"), one to veterans ("american.veterans"), one to feminists ("feminism_tag"), and one to the LGBTQ+ community ("rainbow_nation_us")[7]. The IRA's Instagram activity received 187 million engagements (the total number of comments, likes, reactions, etc.) and its Facebook activity received an additional 76.5 million engagements. New Knowledge comments that Instagram was far more effective in gaining engagements due to its

[6] DiResta, et al., "Internet Research Agency," 14.
[7] DiResta, et al., "Internet Research Agency," 27.

"image-centric" model, which is ideal for waging psychological warfare through memetic content[8]. Additionally, Facebook estimates that over 126 million users were exposed to the IRA's content throughout the campaign through the Facebook platform, and at least an additional 20 million users were exposed to the content through Instagram[9].

It is now necessary to step back and view this from the context of grand strategy and psychological warfare. Clausewitz's trinity of warfare tells us that in order to wage war, any government must maintain the support of its people. If the government loses its legitimacy, then it is at risk of becoming relatively disadvantaged in the global stage due to increased civil dissatisfaction. According to New Knowledge's analysis, the IRA's politically leftist accounts "criticized mainstream, established Democratic leaders as corporatists or too close to neo-conservatives," while politically rightist accounts "denigrated the U.S. media and intelligence community as untrustworthy, and diminished long-standing Conservative [sic] leaders… while elevating Donald Trump"[10]. Both of these viewpoints seek to degrade public trust in the U.S. government and sow social division and tribalism among conservatives and liberals alike, attempting to force the U.S. into a position of relative disadvantage in the context of grand strategy and on the global scale.

A field of military operations that spawned with the creation of the Internet is cyber operations. Our world, at the community, national, and global level, is becoming increasingly dependent on computers. Elections, industrial manufacturing, and even our own personal schedules are facilitated by computing technology. And once scientists at academic institutions started linking computers together for the very first time, individuals began finding ways to use

[8] DiResta, et al., "Internet Research Agency," 8.
[9] DiResta, et al., "Internet Research Agency," 6.
[10] DiResta, et al., "Internet Research Agency," 25.

connections between computers as a medium for destruction. Our adversaries' economies are now increasingly susceptible to cyber attacks through increased dependence on computing.

The cyber domain of warfare was drastically underestimated by national governments on the global scale for almost two decades. The power that cyber superiority carried with it was too difficult to see to be properly understood. Compounded with the novelty of computers and the infancy of the software security industry, open computer networks and the security risks associated with them were not yet well understood. Enter onto the world stage the Rootkit.TmpHider computer worm, better known outside the software security world as Stuxnet.

In January of 2010, a team of inspectors from the International Atomic Energy Agency were investigating an issue in a uranium enrichment plant in Natanz, Iran. Both workers at the plant and experts from the IAEA had recently noticed that the gas centrifuges in the plant had been failing at an extraordinarily high rate[11]. Neither the workers nor the inspectors had any idea what the issue was. The centrifuges controllers ran a specific software which communicated with Siemens Step 7, a controller programming software running on the Windows 7 operating system[12]. Software security experts began to discover over the next couple months that "zero-day" undiscovered exploits was allowing a specific mysterious malware package to infect the Step 7 software and subsequently the centrifuge controllers, causing them to spin the centrifuges at dangerous rates and cause them damage.

A team of experts at Belarusian company VirusBlokAda first discovered the malware programs Rootkit.TmpHider and SScope.Rootkit.TmpHider.2 on June 17, 2010. In an official statement, VirusBlokAda said that the new malware "installs two drivers: mrxnet.sys and mrxcls.sys". These drivers leverage a previously unidentified vulnerability in the way that

[11] Zetter, "Unprecedented Look at Stuxnet."
[12] Tsui, "Stuxnet."

Windows processes shortcut (LNK) files. The malware itself (now referred to as Stuxnet) infected files on a USB flash drive. Plugging the flash drive into a computer and using Windows Explorer to view its contents allowed Stuxnet to leverage the LNK vulnerabilities and infect the current machine. This represented an unprecedented method of attack in the world of computer security. Such a complex operating system as Windows 7 with complex security structures in place was suddenly susceptible to a small executable file that snuck through security to infect a specific distribution of a specific software.

Computer worms were by no means a new idea. For perspective, the first computer worm was the Morris worm[13], which took down about 10% of the infantile Internet in 1988 and decompiled to only a few thousand lines of the C programming language[14]; Stuxnet was detected over twenty years after this incident. But it became clear to computer scientists, software developers, policymakers, and the world at large that this was no ordinary computer worm. Stuxnet was the world's first large-scale digital weapon, created and unleashed into the wild with a specific purpose in its mind. Stuxnet's impact on the world was clear: it damaged or destroyed approximately one thousand Iranian uranium gas centrifuges, which set back their nuclear program by approximately two years[15]. The idea that an intangible weapon, one that existed only in the form of binary, could cause severe damage to a national weapons program by remote control was paralyzing. What seemed once like science fiction suddenly became a reality for the world in 2010.

As with psychological operations, it is important to analyze this not only as a single incident but as one event in the greater context of grand strategy and national power on the global stage. The primary elements of national power are widely considered to be *diplomacy*,

[13] FBI, "Morris Worm."
[14] arialdomartini, "morris-worm."
[15] Tsui, "Stuxnet."

information, *military*, and *economy*. Cyber warfare (and in particular the 2010 Stuxnet attack) targets a country's economy. The ability to cause serious and long-lasting damage to an enemy's industrial complex and war machine from anywhere on the planet, using intangible software to cause tangible effects, is incredibly powerful.

To this day, nobody has positively identified a single organization as the developer of the Stuxnet worm, though many claim the United States government and the Israeli government collaborated to develop it, as both displayed much concern at Iran's growing nuclear program. This claim has not been confirmed or denied in an official capacity by either government. However, the damage that Stuxnet caused to the Iranian nuclear program and therefore Iran's national military strength was unprecedented, and this incident laid bare the power and the dangers of the rising domain of cyber warfare.

But we must recognize that cyber operations are a double-edged sword. As cyber operations become more damaging to our enemies' economic structures, attacks of similar scale become more damaging to our own nation's economic structures. And yet again, our adversaries show no mercy: our own country suffers from threats to our government, to our economy, and to our people originating from throughout the world.

In April 2021, a large-scale cyber attack took down the Colonial Pipeline on the East Coast, shutting down a massive source of oil for millions along the eastern seaboard[16]. On April 29, a hacking group gained access to the networks of Colonial through an unused virtual private network (VPN) account connected to the company's network. Hackers most likely discovered the account's password in a data breach found on the dark web. A little more than a week later, a note appeared on one of the computer screens in Colonial's control room, demanding a ransom payment in the form of millions of dollars in cryptocurrency. Supervisors and executives were

[16] Turton and Mehrotra, "Hackers Breached Colonial Pipeline."

stunned and began to shut down the pipeline in order to protect the company's interests. The steady flow of oil suddenly came to a halt, and the people of the East Coast were suddenly deficient 100 million gallons of oil per day.

In May, Colonial accepted to pay a ransom of $4.4 million and subsequently reopened the pipeline. After an extensive search of several thousand miles of pipeline, executives eventually determined that no pipeline was damaged. After the attack, Colonial consulted the cybersecurity firm Mandiant, which helped Colonial executives to understand the extent of the hackers' damage inside their system. Mandiant determined that the information technology and communications system had been breached, and this was how the hackers were able to post ransom notes and move around inside the Colonial system. However, Mandiant determined that the hackers were unable to breach the operations network: the computer systems that controlled the actual flow of oil through the pipeline, indicating that the damage was not as bad as initially perceived. This supported Colonial's previous conclusion that the pipeline was not directly damaged by the aggressors, serving as a relief to Colonial and to the population of the East Coast as the steady flow of fuel returned.

Arguably more significant than the actual incident to military history and the changing nature of warfare is the unprecedented method of attack and the organization behind it. It is widely believed that the responsible organization is DarkSide, a Russia-linked cybercrime group[17]. Further research into DarkSide reveals that they are not simply petty criminals or genius college dropouts with an advanced understanding of modern operating systems; they are a well-organized group that has found a way to monetize computer system infiltration and convert it into a profitable industry.

[17] Turton and Mehrotra, "Hackers Breached Colonial Pipeline."

The specific form of malware that DarkSide develops is most commonly referred to as *ransomware*, which is software that silently finds its way onto your computer through security bugs in networks, encrypts your files, and offers the user a terrible choice: pay a ransom (typically in the form of cryptocurrency) within an allotted time limit or lose their files forever. DarkSide offers ransomware-as-a-service (RaaS), meaning they develop ransomware for affiliate organizations and clients and distribute the software for profit[18]. And the methods by which DarkSide infiltrates computers is incredibly complex and nuanced. DarkSide ransomware is the result of careful engineering and development, and it is clear that the software has specific intentions in mind. For example, on initialization, DarkSide ransomware will check the system language to ensure that the host machine is not owned by a Russian-affiliated organization[19]. This, in addition to the list of locations that DarkSide most commonly attacks, indicates that the cybercrime group seeks to attack computer networks operated by English-speaking organizations.

The implications of the recent DarkSide ransomware attack towards U.S. national security are not to be underestimated. First of all, the method of DarkSide's operation reveals that cyber warfare (and specifically ransomware) is now becoming an industry; a commodity bought and sold by cyber criminal groups that can be modified to suit a client's needs. This stands in stark contrast to computer malware as a toy made by a bored college student (as it was in the case of the Morris worm) or a weapon developed by a well-funded organization with a specific target in mind (as in the case of Stuxnet). And more significantly, DarkSide's behaviors reveal that English-speaking (and potentially American) countries, organizations, and individuals are being specifically targeted by these criminal groups. It is unknown if DarkSide is endorsed

[18] Yogesh, "DarkSide Ransomware."
[19] Shimol, "Return of the Darkside."

or funded by the Russian government or the Internet Research Agency, although it is clear that DarkSide has intentions to damage United States economic structures and weaken the United States government.

It is also important to consider this attack, like the others above, in the context of grand strategy. A strong economy, one of the four previously discussed elements of national power, is critical to supporting the government, the military, and the people through Clausewitz's trinity of war. By grinding to nearly a complete halt a significant means of oil transportation, we see that DarkSide (and whoever their ransomware client may have been) has a new capability of severely damaging the U.S. economy, which has had and may continue to have obvious and far-reaching negative impacts on military production, civilian welfare, and government operation. Furthermore, such attacks can be used to wage psychological warfare on the U.S. population; if our economic infrastructure is vulnerable to attack, then citizens are less likely to trust the United States government and less likely to support the Department of Defense's operations. It is for both this reason and the need for economic stability that the United States remains particularly susceptible to cyber warfare.

Warfare is the use of force to force an adversary to comply with one's demands or will. And due to our nation's increased dependence on and susceptibility to psychological operations and cyber operations, warfare's defining act of force and thus its very nature has changed dramatically over the last twenty years. We have seen through the Internet Research Agency's ruthless psychological warfare campaign during the 2016 election cycle that psychological operations are a largely unexplored new threat to our national security. The Internet makes psychological operations extraordinarily inexpensive; any organization can easily create a couple dozen social media accounts with different names and target audiences and use them to broadcast

an endless stream of carefully engineered information and opinions to the American population. And a dangerous complement to psychological operations in the information age is cyber warfare; this was made quite clear through both the Stuxnet and DarkSide attacks on the Iranian nuclear program and U.S. fuel infrastructure, respectively. Again, the Internet makes inflicting damage on enemy economic infrastructure much easier, much less expensive, and much more discreet. A malicious program can be sent as a few packets of unassuming data over a vast network, lying silent in every machine it infects until it finds its target. As the Internet, social media, and cybersecurity are in their relative infancy, still experiencing growing pains as they find their place in our society, the next twenty years will hold new hopes, new challenges, and new threats for our world. In the meantime the only thing we as a nation can do is learn from our own and others' weaknesses and mistakes of the past so that we may stand more prepared to defend ourselves when the time comes, whether that time be tomorrow or in the distant future.

Bibliography

arialdomartini. "morris-worm." GitHub (Git repository). Last commit November 24, 2020. https://github.com/arialdomartini/morris-worm

Clausewitz, Carl von. *On War*. Princeton University Press, 1976.

Department of the Army. *ATP 3-13.1: The Conduct of Information Operations*. Washington, D.C.: Department of the Army, 2008.

DiResta, Renee, Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Jonathan Albright, and Ben Johnson. "The Tactics & Tropes of the Internet Research Agency." *University of Nebraska - Lincoln*, 2019, https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1003&context=senatedocs

Federal Bureau of Investigation. "Morris Worm, The." Federal Bureau of Investigation News. Last modified November 2, 2018. https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218

Thompson, Nicholas, and Issie Lapowsky. "How Russian Trolls Used Meme Warfare to Divide America." *Wired*, December 17, 2018. https://www.wired.com/story/russia-ira-propaganda-senate-report/

Patil, Yogesh. "DarkSide Ransomware." Qualys Community. Last modified June 9, 2021. https://blog.qualys.com/vulnerabilities-threat-research/2021/06/09/darkside-ransomware

Roser, Mark, Hannah Ritchie, and Esteban Ortiz-Ospina. "Internet." Our World In Data, n.d. https://ourworldindata.org/internet

Shimol, Ben Snir. "Return of the Darkside: Analysis of a Large-Scale Data Theft Campaign." Varonis: Inside Out Security. Last modified March 18, 2021. https://www.varonis.com/blog/darkside-ransomware

Tsui, Sabrina. "Stuxnet." Dangerous World. Last modified December 12, 2018. https://dangerousworld.soe.ucsc.edu/author/sctsuiucsc-edu/

Turton, William and Kartikay Mehrotra. "Hackers Breached Colonial Pipeline Using Compromised Password." *Bloomberg*, June 4, 2021. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

Zetter, Kim. "An Unprecedented Look at Stuxnet, the World's First Digital Weapon." *Wired*, November 3, 2014. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/