Violent Limitation: Cyber Effects Reveal Gaps in Clausewitzian Theory

Major David Greggs

ABSTRACT

The theoretical foundation remains fundamental to U.S. military policy and doctrine. Carl von Clausewitz provides the core understanding of war and warfare in U.S. military doctrine. As a result, the U.S. military describes and understands war within the Clausewitzian frame of physical violence to accomplish a political goal by enforcing will on the military of an opposing state through physical actions. However, the cyber domain and the effect of cyber actions reveal that our understanding of war can no longer be restricted to the Clausewitz paradigm.

Cyber effects can cause destruction without kinetic actions. The cyber domain's emergence has brought the cognitive dimension to the forefront of many military leaders' and planners' thinking. Cyber activities reveal that while new technology may not have changed war, a theoretical foundation built upon Clausewitz restricts the understanding of war too narrowly for the modern era.

The theoretical references within U.S. military policy and doctrine are no longer sufficient to provide an understanding of war. War is more than just physical violence, but military policy restricts war to just that. This research reveals that U.S. military leadership may need to adopt new or additional theoretical references that encompass all domains of modern war.

This is a work of the U.S. Government and is not subject to copyright protection in the United States. Foreign copyrights may apply.

David Greggs is a Major in the U.S. Army. He is a cyber operations officer with a background in intelligence. He has deployed to Afghanistan and completed a Master's Degree in Information Technology Management. He is also a graduate of the Advanced Military Studies Program and the Command and General Staff College.

INTRODUCTION: AN INSUFFICIENT THEORY

Cyberattacks remain a significant and growing risk, with the potential for increasing cost, scope, scale, and physical consequences. As costs due to cyber incidents increase, and the United States spends billions on cyber security, the question arises, why has the U.S. not committed to fighting cybercrime or cyber terrorism as it did after September 11?[1] Why are cyberattacks not viewed the same as physical attacks, regardless of the damage they cause? The problem lies in the insufficient theoretical foundation on which U.S. military leaders and planners rely.

These theoretical considerations serve a critical and implicit role in shaping U.S. military policy and doctrine. They shape how senior leaders think about war and the assumptions regarding how it should be carried out – even what constitutes war. They are largely based on an old collection of theoretical references that provide the foundation for the development of today's policies and doctrine. Our U.S. national security and military policies then draw on these theories to conceptualize what war is and how it should be conducted. These theories in turn provide the basis for the development of military doctrine which dictates how military forces should think about and approach warfare. Thus, this paper examines the theoretical references within U.S. military policy and doctrine and concludes that the theoretical references that shape military leaders' and planners' assumptions, conceptions, and practices are insufficient to provide for a war theory that incorporates the cyber domain.

U.S. doctrine often cites such theorists as Carl Von Clausewitz, Sun Tzu, Thucydides, and Alfred Thayer Mahan. These war theorists, but especially Clausewitz, continue to shape U.S. military policy and doctrine, yet their ideas poorly conceptualize war in the cyber age. Warfare has changed dramatically from the era of swords, muskets, and battleships to today, and while cyber may not have fundamentally changed the nature of war, it has fundamentally altered the conduct of war. The cyber domain may continue to serve primarily as an enabler for other domains. However, cyber can also deliver effects historically restricted to the physical domains. If there is a particular effect required, cyber can likely accomplish it.

This paper explores U.S. military policy and doctrine to provide a U.S.-centric understanding of war and warfare. It then explores the limits of the U.S. understanding of war and warfare and defines how cyber may or may not fit within those boundaries. Then, through historical examples, the paper explores how the cyber domain can result in effects traditionally associated with kinetic actions in warfare, concluding that the theoretical foundation in U.S. military policy and doctrine is inadequate, insufficient, and remains too restrictive for today's U.S. military leaders and planners.

The Foundation: Theoretical References in U.S. Policy and Doctrine

Theory serves as the critical component to support the thought processes of senior military leaders and planners. Theory undergirds how senior leaders and planners respond as a nation faces war, where chance and chaos persist. Today, U.S. military doctrine and policy draw their theoretical foundation almost exclusively from the Napoleonic period and its most prolific theorist, Carl Von Clausewitz. This exclusivity, drawing on a fixed point in time, has prevented a broader examination of modern warfare. If war never changed, this might not matter. But the technology, equipment, tactics, and essential practice of war do change. War looks different today than it did in the past.

Joint Publication (JP) 1 Volume (Vol) 1, Joint Warfighting provides overarching guidance and delivers fundamental principles for the employment of the Armed Forces of the United States.[2] This capstone publication also bridges other policy documents, such as the National Security Strategy (NSS) and the National Defense Strategy (NDS), and serves as the foundation for other publications.[3] As such, JP 1 Vol 1 is one of the most significant and consequential manuals for the U.S. Armed Forces.

Yet, this capstone doctrine only allots minimal space for discussion on the theory of war and only refers to a single theorist, Carl von Clausewitz, as a reference for understanding and describing war. JP 1 Vol 1 states that "the nature of war is immutable,"[4] describing it as a "violent clash of wills" characterized by the trinity of forces of emotion (passion), chance, and reason.[5] Clausewitz further described war as an act of violence to compel an enemy to do the will of the friendly state, and ultimately a "continuation of politics by other means," an idea that this document affirms.[6] In sum, JP 1 Vol 1—the foundation of U.S. military doctrine—describes war as physical violence toward achieving a political objective to enforce will on an enemy. JP 1 Vol 1 also describes warfare as the "the how," or ways, of waging armed conflict.[7] It may also be called the character of war. New technologies and domains do not change the nature of war, but they alter how it is conducted.[8] Yet the Clausewitzian conception of warfare focuses on physical violence as the means of war, equating the destruction of the enemy military force or conquering territory with defeating the enemy overall.[9] Despite dramatic changes in technology and the world since Clausewitz's *On War*, these concepts find a home in doctrine. JP 1 Vol 1 describes defeating enemy forces through attrition and annihilation.[10] Considering two types of warfare, conventional and irregular, both remain armed forces-centric and physical violence-centric.[11]

Service-specific doctrine echoes joint doctrine in its foundational references. Air Force Doctrine Publication 1, the Air Force capstone publication, cites Clausewitz to describe war as an "extension of politics by other means."[12] The U.S. Navy follows suit in its capstone publication by citing Clausewitz to describe the art of war and using naval means in combat, asserting the naval domain as primary.[13] Similarly, U.S. Army doctrine also references Clausewitz but maintains the decisive nature of the land domain. Ultimately, joint and service doctrine publications remain restricted to very few theoretical references but overwhelmingly focus on Clausewitz and his description of war to serve as the foundation.

While U.S. policy documents such as the NSS and the NDS do not specifically cite theorists, when addressing modern threats like cyberattacks, these strategic documents muddy the waters, confusing rather than clarifying the issue. The 2017 NSS distinguished between cyber and physical threats, while acknowledging that cyberattacks are a feature of modern conflict, and actions may occur in cyberspace without physical border crossings.[14] The 2022 NSS builds on these concepts and acknowledges that international law applies both online and offline.[15] However, while acknowledging state-sponsored actors may extort citizens or attack critical infrastructure through cyber means, the idea of war remains absent from the conversation. The 2022 NDS recognizes that China may leverage the cyber domain in joint warfare but ignores the possibility that effects may take place in the cyber domain independent of other domains.[16]

U.S. policy treats cyberspace as an enabler or supporter of war, but incapable of war in and of itself. Cyberattacks persist, but U.S. policy does not acknowledge cyberattacks in the same way as physical attacks. The result is that the U.S. strategic documents disconnect physical effects from cyber activities and capabilities.[17] This strategic formulation separates the means of creating the effects from the effects themselves and elevates how an activity takes place to greater importance than the impact of that action. Military policy and doctrine are the documents to which planners, strategists, and decision-makers refer, but the theoretical foundation remains fundamental.

On Violence: Clausewitz and U.S. Policy Agree

Carl von Clausewitz provides the reader an opportunity to think about war at varying and increasing levels of complexity, building on the idea that war is a simple duel to the understanding of war as part of a more complex political discourse and an extension of politics. He also provides a complex trinity where passion, chance, and reason all work in concert and in opposition with one another as he describes war. While Clausewitz acknowledges the complexity and variety of inputs to war, he ultimately describes war as basic physical violence. It is this framing of war by Clausewitz and now by U.S. military leadership, strategists, and warfighters that ignores other possibilities and the learned experiences of recent conflicts in which cyber has played a pivotal role in shaping the battlefield, supporting the warfighter, and even achieving political objectives. Furthermore, this implies that if the objective can be reached without violent action, perhaps these other means would be preferable and less costly to the attacker. Additionally, if the conception of the nature of war—that is, politically centric and exclusively physically violent—does not change and Clausewitz was correct, then new discussion on the nature of war serves little purpose. However, as we have seen, warfare involving cyberspace with today's modern equipment looks vastly different than the warfare Clausewitz observed in 1800.

As an example, in 2007, Estonia was preparing to move a WWII memorial statue that had been in place for 70 years. In protest of the movement, attackers conducted cyberattacks against Estonian government resources and the banking system for 22 days. This event continues to drive considerations of state sovereignty in cyberspace, a topic exacerbated by the lack of an accepted cyber border.[18] Regardless of whether the attackers were state-sponsored or not, the cyberattacks demonstrated the capabilities to disrupt or destroy government operations to motivate political action without physical violence.[19]

Limiting the concept of war to physical violence narrows the basic understanding of war and warfare while also failing to capture the diverse capabilities and effects that occur in war beyond the physical. Of particular interest are those activities that occur within and against belligerents' minds and the possibility for cognitive influence. War itself has always been about more than the destruction of material things and violence remains just a means to an end.[20] Antulio Echevarria said it simply enough: "The essence of war may be the violent clash of arms, but war itself is much more."[21] While war is usually violent, strategy requires more than just the application of violence and destructive force.[22] Violence is not a principle of war. Yet, unfortunately, that is how Clausewitz is often read and interpreted.

To be clear on this point, the nature of war has not suddenly changed, but rather the Clausewitzian description and understanding of war is not adequate for today. The cyber domain has revealed that it is possible to have corporal effects without physical violence, and cognitive effects by changing minds without employing violent means. The cyber domain and the new character of war reveal just how inadequate Clausewitz's description of the nature of war is today.

Cyber Incidents Revealing New Possibilities in the Character of War

Just as no one goes to war for war's sake; no one hacks something for the sake of hacking.[23] Cyberattacks can cause direct physical destruction in addition to indirect disruption and confusion. However, the primary destructive effect of an attack may matter much less than the second and third-order effects. How that happens might look different than what many people are used to.

By examining several historical events, this paper will demonstrate that cyber effects can cause the same or similar effects as traditional kinetic munitions. These incidents demonstrate that acts of warfare are better recognized by their effects than their causes. In addition, it is possible to influence an adversary's strategies, policies, and decisions without taking physical actions altogether.

Stuxnet – A Precision Time Delayed Bomb

The Stuxnet incident, discovered in 2010, was like a bomb in place at least one year before being found, and only after it had done irreparable damage.[24] Symantec, a global cybersecurity company, described Stuxnet as a complex threat with dramatic real-world implications and a "type of threat we hope to never see again."[25] This virus was even called a "cyber missile" after it caused extensive physical damage by destroying approximately 1,000 centrifuges within Iran's Natanz nuclear facility. [26]

Stuxnet was one of the most complex pieces of malware ever developed when it was deployed, resulting in the infection of 100,000 hosts in 155 countries.[27] Notably, the additional infections were unintentional and more due to the nature of the complexity of the Stuxnet virus and its coding to seek out vulnerable targets.[28] Computer worms can self-propagate and infect many more hosts than originally intended, much like one of the first computer worms did in 1988.[29]

Stuxnet resembled a living biological weapon. The Stuxnet virus self-propagated and exploited four vulnerabilities before infecting thousands of computers.[30] It also demonstrated how a cyberattack could be successful even if the exact physical location of the victim is unknown, something impossible with physical bombs.[31] This fact does not eliminate geography as a significant factor but certainly changes how geography can be understood and what limiting factors may or may not exist. When Clausewitz spoke of geography, he assumed the weeks or months it might take to move an army from one theater to another.[32] With Stuxnet, physical geography ceased to be a limiting factor as it wreaked havoc on Iranian centrifuges irrespective of distance.

The attack caused Iran to halt its nuclear program at Natanz, and it took a year for Iran to recover the losses from the attack.[33] Stuxnet was a precision weapon that caused physical and psychological damage far beyond the initially intended victim in a way that resembles a living and thinking weapon.[34] No state has officially taken responsibility for Stuxnet, but allegations persist that it was a combination of the United States and/or Israel.[35] The complexity of Stuxnet alone led Symantec to believe that only a few attackers could produce a threat like it.[36] Stuxnet remains critical for examination because of the amount of physical damage done, and the politically connected effect of preventing Iran from becoming a nuclear power.

There are differences in means, but the damage is similar to the effects from physical warfare. The attack took place a year or more before the effect was felt, which has changed the conception of the calculus of time and space resulting from a cyberattack. The quantitative damage was not immediately apparent, while the qualitative damage persists today. This challenges the meaning and understanding of surprise.

NotPetya

In June 2017, Russia conducted a cyberattack against Ukraine that was perhaps the most destructive and costly to date.[37] Known as "NotPetya" because analysts initially thought that the virus was avariation of an older "Petya" ransomware virus from 2016.[38] NotPetya caused more damage than the previous virus because it took advantage of a Windows vulnerability and encrypted the hard drives of the infected computers.[39] With ransomware, the victim can usually pay money to get the password to unlock their computer. But with NotPetya, there was no way to unlock the infected machines.[40]

The White House called NotPetya a Russian, and specifically Kremlin, effort to destabilize Ukraine.[41] The UK Government echoed the U.S. statement and even said that Russia had violated Ukrainian sovereignty.[42] The Russian government disrupted Ukrainian systems, effectively destroying hard drives, and made the computers inoperable and unusable until the victims acquired new hard drives and installed the required software.[43] Cost estimates for NotPetya were over $10 billion.[44]

The international shipping organization Maersk had so many computers affected by the virus that their capability to move cargo—one-fifth of worldwide shipping—was disrupted and nearly stopped due to the virus.[45] Merck Pharmaceuticals lost 15,000 computers to the virus, and the attack cost them $870 million.[46]

In all, the NotPetya attack caused billions of dollars in damage, disrupted global supply, and effectively destroyed up to 10 percent of all computers in Ukraine.[47] This computer-based non-kinetic and non-physical attack further demonstrates the destructive capability of cyberattacks, the extensive costs associated with such attacks, and the ripple effects that a significant cyberattack can have. The United States and its critical infrastructure were not targeted or damaged by NotPetya, but an attack in 2021 would change that.

Cyberattacks: The Shockwave May Reach Unintended Victims

The WannaCry ransomware virus attack in 2017 highlighted new possibilities when the cyberattack infected over 230,000 computers and reached 150 countries in just one day.[48]

Although individuals could recover their computers by paying $300 in Bitcoin to retrieve the password and get their computers back, WannaCry was not a simple ransomware virus.[49] Notably, the WannaCry attack directly affected hospitals. The attack prevented doctors from seeing patient data or recording medication changes. Patients missed surgeries because doctors could not access their systems to approve them.[50] Caregivers could not monitor even the most critical patients due to lost computer access.[51] Medical equipment like X-ray machines may not be running a Windows system, but the computer to read the X-ray was, which limited the doctors' ability to read the image.[52] Doctors in British hospitals even canceled surgeries or turned patients away altogether.[53]

In 2020, another ransomware attack—this one relatively minor—targeted a hospital in Düsseldorf, Germany, which crashed computer systems.[54] As a result, a woman who was sent to another hospital much further away died in transit.[55] The attacked hospital may not even have been the primary target, and the woman who died almost certainly was not the target.[56] If a future attack were crafted to cause death, it requires little imagination to envision that real possibility from happening. This type of attack was impossible only a few years ago, much less in the 1800s when Clausewitz wrote *On War*.

Colonial Pipeline

The Texas-based Colonial Pipeline cyberattack in 2021 was significant because it was an attack against U.S. critical infrastructure.[57] The attack began on May 7, 2021, and the company shut down its operations until May 13, 2021.[58] Some of the digital control systems were infected, and shutting down operations caused gas shortages and a dramatic rise in fuel prices.[59]

Darkside, the group that claimed responsibility for the attack, said that its "goal is to make money and not create problems for society."[60] Darkside accomplished its goal when Colonial Pipeline paid a $5 million ransom the day after the attack.[61] However, the psychological (cognitive) effects were more relevant and long-lasting. Many U.S. citizens panicked. People bought containers and filled fuel tanks as they feared fuel shortages.[62] While the attack and its physical effects did not last long, and the pipeline was only shut down for a matter of days, the amount of fear created in that short period was remarkable. The emotional and mental effects remain the most critical factors.

Cyberattacks Cause Physical and Cognitive Disruption and Destruction

As the Stuxnet attack demonstrated, cyber effects can reach equipment or devices on a network and destroy them, regardless of whether the network connects to the internet.[63] Critical infrastructure can be exploited and destroyed through cyberspace, though physical destruction may not be required. In 2021, an attacker hacked into a water treatment plant in Florida, making the water unsafe to drink.[64] What we see is the potential in warfare for cyberattacks against critical infrastructure to create destruction and confusion in areas once considered sanctuaries. Such deep attacks into enemy territory could involve power loss across a city, including hospitals, water and sewage treatment, and infrastructure destruction—all without any traditional physical actions. More, not fewer, civilians will be at risk.

Confusion and disruption that spreads beyond the realm of the conventional battlefield are not future threats; they are possible now. This type of warfare would not look like a war Clausewitz wrote about, but it would be war nonetheless. More importantly, these effects could go on for months before a traditional attack happens. As a result, the U.S. could be under attack before any U.S. leader or planner realizes what is happening.

Examining just a few cyberattacks and their effects brings several things to the forefront. First, cyberattacks can cause physical destruction. Second, cyberattacks can cause tactical effects such as disruption and degradation of operations. Third, cyberattacks can cause death. The computer virus itself does not kill anyone, but the connection remains clear. Finally, and perhaps most importantly, cyberattacks can have significant and deep psychological and emotional effects. Cyberattacks can make people afraid and disrupt an individual's rational thinking.

War and Cyber Violence

While war will likely always include physical violence, war does not exclusively involve violence. This is not new, but violence is the primary focus Clausewitz and U.S. military doctrine account for in the nature of war. Nation-states only consider war and the use of violence to get something they want.[65] Political discussion can transition from a friendly negotiation to strongly worded letters and ultimately to the point where one or both sides feel it necessary to negotiate violently, including killing or destroying to bring about a resolution. To the contrary, Thomas Rid argues in his book *Cyber War Will Not Take Place* that violence is a prerequisite for war, so cyberattacks will never be the same as physical attacks.[66]

However, war is not about physical violence but is about the political objective: the original reason for escalating from negotiation to war, the act of forcing an opponent to bend their will. Dr. Aaron Brantly stated in his article, "The Violence of Hacking: State Violence and Cyberspace," that restricting the consideration of violence to the physical world ignores the impact of other manifestations of violence that achieve strategic, operational, and tactical objectives that were once only achievable through physical means.[67] Indirect attacks and cyberattacks can affect an enemy system and support achieving goals across the spectrum of conflict. Dr. Brantly stated that "when a murder occurs, police do not absolve the murderer if he used a gun. Despite the disconnect in both physical and temporal space between the action, pulling the trigger, and the effect, a bullet entering and harming a victim, the two parts of the causal chain are linked inexorably."[68] The impact of something remains more important to consider because it recognizes that not all attacks involve traditional armed violence.[69]

The lack of physical violence in a cyberattack, a consistent inclusion in “traditional” war, could imply that cyberwar is simply not war. However, as this paper has already demonstrated, cyber effects can cause destruction and death without physical means. Even if a war must always involve violence, cyberattacks can also fulfill that requirement. Cyberattacks can be physically, logically, or cognitively destructive.

Since there has not been a global war in recent years, observers have yet to see the full range of what cyberattacks may accomplish when world powers are pressed to leverage those capabilities across the full spectrum of operations. While it may be that a cyberattack will not physically blow up an enemy system, it could disable its firing mechanism or targeting computer.[70] If a tank gets destroyed because of cyber-enabled operations, it does not matter how it happened. Just as muskets increased the range of direct fire and nuclear weapons increased the destructive power of bombs, cyberspace expanded the deadly potential and distance forces may reach.[71] Cyber can affect other domains, but it can also broaden other capabilities.

The nature of war itself remains a competition that involves many disparate factors. In past wars, opposing forces targeted civilian support infrastructure with military forces, such as ball-bearing plants in Germany during WWII. It would be no surprise for home station power, water, and logistic networks to come under a cyberattack in modern war. Rather than consider whether violence occurs in cyberspace or if the information dimension should or could constitute violence, the effects of action must remain of primary consideration.

CONCLUSION

U.S. policy and doctrine rely on a war theory that remains incapable of explaining the modern character of war, in particular cyberwar. Today’s doctrine relies heavily on Clausewitz and his relatively narrow description of war and warfare that the modern possibilities of warfare barely make sense when viewed through a Clausewitzian lens. Due to doctrine and policy's overt and overwhelming reliance on Clausewitz, his descriptions remain the ripest for criticism.

Clausewitz within his framing of war does not fully account for cyber operations or their capabilities. Nor does he adequately capture the dramatic change in how forces can traverse physical geography, the criticality of computer network logical geography and how it connects systems, or an appreciation for a systemic effect beyond a singular physical center of gravity. Clausewitz also does not fully capture the importance of information warfare and its application to changing an enemy's will.

War should not be reduced to merely physical violence, which unfortunately remains largely how U.S. policy and doctrine conceptualize war. As has been demonstrated, cyber effects can exert warfare wholly apart from kinetic actions. Clausewitz and military policy do not account for this fact. The rise of the cyber domain also reveals the importance of the information dimension and the preeminence of influencing the minds of decision-makers.

Furthermore, today's leaders should avoid the temptation to re-interpret Clausewitz to modernize him or his theory. Today's doctrine and policy related to war should be firmly rooted in theory informed by an understanding of war and warfare that accurately captures the effects of all domains. The nature of war is complex. U.S. policy and doctrine provide a simple and woefully inadequate description. The current theoretical references within doctrine and policy need to expand to capture a greater range of ideas about war. Theory should overcome this ambiguity with principles, fill knowledge gaps, and enable action when unknowns persist. With current theory firmly anchored in Clausewitz, removed from the cyber domain, and wholly disconnected from the complexity of modern systems, senior military leaders and planners have little to rely on to provide fundamental knowledge when a crisis occurs.

Anchoring on Clausewitzian theory serves to limit the U.S. military's understanding of war to industrial-age ideas and fails to account for two essential truths. First, war is about more than physical violence. Second, cognitive effects in warfare may be as or more important than physical effects. U.S. policy and doctrine narrowly focus on war as an act of violence, specifically physical violence, against military forces. This idea has been repeated so often that it is ingrained in U.S. policymakers, senior military leaders, and planners.

Leaders must concern themselves with the war that will be fought in the future: The next war. Yet our thinking largely remains rooted in the past. With such a focus, U.S. policy and doctrine lack a theoretical foundation to accurately and holistically describe the nature of war that is relevant and complete enough for the current possibilities in the character of war. As a result, the United States and its allies are not well-positioned to recognize the next war when it comes, or to appreciate the nuances and intricacies of warfare before it is too late.

DISCLAIMER

The views expressed here are those of the author alone and do not necessarily represent the views, policies, or positions of the U.S. Government, Department of Defense or its components, to include the Department of the Army, or the United States Military Academy.

NOTES

1. Steve Morgan, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," *Cybercrime Magazine*, January 18, 2022, Accessed October 8, 2021, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.; Cybersecurity & Infrastructure Security Agency, "Cost of a Cyber Incident: Systematic Review and Cross-Validation," 1-146, October 26, 2020, Accessed January 18, 2022, https://www.cisa.gov/sites/default/files/publications/CISA-OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf, 12.
2. US Department of Defense, Joint Staff, Joint Publication (JP)1 Volume 1, *Joint Warfighting*, (Washington DC: Government Publishing Office, 2023), xiv.
3. US Joint Staff, JP 1 Volume 1 (2023), vi-vii.
4. US Joint Staff, JP 1 Volume 1 (2023), viii, II-14
5. US Joint Staff, JP 1 Volume 1 (2023), II-10-II-12
6. Carl von Clausewitz, *On War*, (Oxford University Press, 2007), 75, 87; US Joint Staff, JP 1 Vol 1 (2023), viii, II-10.
7. US Joint Staff, JP 1, Volume 1 (2023), II-5.
8. Nicholas Michael Sambaluk, *Myths and Realities of Cyber Warfare: Conflict in the Digital Realm*, (Santa Barbara: Praeger, 2020), 2.
9. Clausewitz, *On War*, 75, 94.
10. US Joint Staff, JP 1, Volume 1 (2023), III-15.
11. US Joint Staff, JP 1, Volume 1 (2023), II-6-II-7.
12. US Department of the Air Force, Air Force Doctrine Publication (AFDP) 1, *The Air Force*, (Washington DC: Government Publishing Office, 2021), 1; Clausewitz, On War, 87.
13. US Department of the Navy, Naval Doctrine Publication (NDP) 1, *Naval Warfare*, (Washington DC: Government Publishing Office, 2020), 33.
14. United States, "National Security Strategy of the United States of America," President of the United States, (Washington DC: Government Publishing Office, 2017), 12, 23, 31.
15. President of the United States, National Security Strategy, 34.
16. President of the United States, National Security Strategy, 4, 6.
17. President of the United States, National Security Strategy, 18.; Department of Defense, "Summary: Department of Defense Cyber Strategy," (Washington DC: Government Publishing Office, 2018), 7; United States, "National Security Strategy of the United States of America," 23.; United States, "National Security Strategy of the United States of America," President of the United States, (Washington DC: Government Publishing Office, 2017), 4.
18. Herzog, Stephen. "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." Journal of Strategic Security 4, no. 2 (2011): 49–60, Accessed June 28, 2023, http://www.jstor.org/stable/26463926., 50.; David Greggs, "Asserting a Cyber Border," Real Clear Defense, April 8, 2023, Accessed June 28, 2023, https://www.realcleardefense.com/articles/2023/04/08/asserting_a_cyber_border_892656.html.
19. Herzog, "Revisiting the Estonian Cyber Attacks," 60.
20. David Lonsdale, "*Clausewitz in the Twenty-First Century*," ed. by Hew Strachan, & Andreas Herberg-Rothe, (Oxford: Oxford University Press, 2007), 247.
21. Antulio J. Echevarria, "Preparing for One War and Getting Another?," Strategic Studies Institute, US Army War College, September 1, 2010, Accessed February 22, 2023, https://www.jstor.org/stable/resrep11589., 25.
22. Lonsdale, *Clausewitz in the Twenty-First Century*, 247.
23. Clausewitz, *On War*, 80-81, 87.
24. Falliere et al., *W32.Stuxnet Dossier*, Symantec Security Threat Report, (Cupertino, CA: Symantec, 2010), 1-64. Accessed February 22, 2023. https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf., 2.
25. Falliere et al., *W32.Stuxnet Dossier*, 50.
26. Michael Holloway, "Stuxnet Worm Attack on Iranian Nuclear Facilities," July 16, 2015, Accessed February 22, 2023, http://large.stanford.edu/courses/2015/ph241/holloway1/; David E. Sanger, *The Perfect Weapon*, (New York: Crown Publishing, 2018), 41-42.; Mark Clayton, "How Stuxnet cyber weapon targeted Iran nuclear plant," *Christian Science Monitor*, November 16, 2010, Accessed February 22, 2023, https://www.csmonitor.com/USA/2010/1116/How-Stuxnet-cyber-weapon-targeted-Iran-nuclear-plant.
27. Falliere et al., *W32.Stuxnet Dossier* 1, 5-6.

NOTES

28. Falliere et al., *W32.Stuxnet Dossier* 1, 7.

29. "The Morris Worm," Federal Bureau of Investigation, November 2, 2018, Accessed February 22, 2023, https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218.

30.Falliere et al., *W32.Stuxnet Dossier*, 2.

31. "Better than bunker busters: The virtual Chinese water torture," Langner, November 15, 2010, Accessed February 22, 2023, https://www.langner.com/2010/11/better-than-bunker-busters-the-virtual-chinese-water-torture/.; Clayton, "How Stuxnet cyber weapon targeted Iran nuclear plant."

32. Clausewitz, *On War*, 214.

33. Sanger, *The Perfect Weapon*, 41-42.

34. Sanger, *The Perfect Weapon*, 42.

35. Josh Fruhlinger, "What is Stuxnet, who created it and how does it work?," CSO, August 31, 2022, Accessed February 22, 2023, https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html.

36. Falliere et al., *W32.Stuxnet Dossier*, 50.

37. "Statement from the Press Secretary," Press Secretary, White House, February 15, 2018, Accessed Accessed February 22, 2023, https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/.

38. Josh Fruhlinger, "Petya ransomware and NotPetya malware: What you need to know now," CSO, October 17, 2017, Accessed February 22, 2023, https://www.csoonline.com/article/3233210/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html.

39. Ivan Belcic, "What is Petya Ransomware, and Why is it so Dangerous?," Avast, September 21, 2021, Accessed February 22, 2023, https://www.avast.com/c-petya.

40. Belcic, "What is Petya Ransomware, and Why is it so Dangerous?"

41. "Statement from the Press Secretary," Press Secretary.

42. "Russian military 'almost certainly' responsible for destructive 2017 cyber attack," National Cyber Security Centre, February 14, 2018, Accessed February 22, 2023, https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack.; "Foreign Office Minister condemns Russia for NotPetya attacks," Foreign Office Minister Lord Ahmad, February 15, 2018, Accessed February 22, 2023, https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks.

43. Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," Wired, August 22, 2018, Accessed February 22, 2023, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

44. Carly Burdova, "What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant?," Avast, October 1, 2021, Accessed February 22, 2023, https://www.avast.com/c-eternalblue#topic-2.

45. Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History."

46. Nica Latto, "What is WannaCry?," Avast, August 25, 2021, Accessed February 22, 2023, https://www.avast.com/c-wannacry.

47. Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History."

48. Carly Burdova, "What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant?," Avast, October 1, 2021, Accessed February 22, 2023, https://www.avast.com/c-eternalblue#topic-2.

49. Nica Latto, "What is WannaCry?," Avast, August 25, 2021, Accessed February 22, 2023, https://www.avast.com/c-wannacry.

50. Burdova, "What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant?."

51. Andy Greenberg, "How the Worst Cyberattack in History Hit American Hospitals," Slate, November 5, 2019, Accessed February 22, 2023, https://slate.com/technology/2019/11/sandworm-andy-greenberg-excerpt-notpetya-hospitals.html.

52. Greenberg, "How the Worst Cyberattack in History Hit American Hospitals."

53. Melissa Eddy and Nicole Perlroth, "Cyber Attack Suspected in German Woman's Death," *NY Times*, September 18, 2020, Accessed February 22, 2023, https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html.

54. Eddy and Perlroth, "Cyber Attack Suspected in German Woman's Death."

NOTES

55. Eddy and Perlroth, “Cyber Attack Suspected in German Woman’s Death.”

56. “First Death from a Cyberattack Reported in Germany,” Chivaroli Insurance, October 6, 2020, Accessed February 22, 2023, https://chivaroli.com/first-death-from-a-cyberattack-reported-in-germany/.

57. “Pipeline,” Cybersecurity & Infrastructure Security Agency, Accessed November 17, 2021, https://www.cisa.gov/key-words/pipeline; “Critical Infrastructure Sectors,” Cybersecurity & Infrastructure Security Agency, Accessed February 22, 2023, https://www.cisa.gov/critical-infrastructure-sectors; “Energy Sector,” Cybersecurity & Infrastructure Security Agency, Accessed February 22, 2023, https://www.cisa.gov/energy-sector.

58. “Colonial Pipeline Cyber Incident,” Office of Cybersecurity, Energy Security, and Emergency Response, Accessed February 22, 2023, https://www.energy.gov/ceser/colonial-pipeline-cyber-incident.

59. Sean Michael Kerner, “Colonial Pipeline hack explained: Everything you need to know,” TechTarget, April 26, 2022, Accessed February 22, 2023, https://whatis.techtarget.com/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know; Brian Fung, “Colonial Pipeline says ransomware attack also led to personal information being stolen,” CNN, August 16, 2021, Accessed February 22, 2023, https://www.cnn.com/2021/08/16/tech/colonial-pipeline-ransomware/index.html.

60. Mary-Ann Russon, “US fuel pipeline hackers 'didn't mean to create problems,'” BBC, May 10, 2021, Accessed February 22, 2023, https://www.bbc.com/news/business-57050690.

61. Christina Wilkie, “Colonial Pipeline paid $5 million ransom one day after cyberattack, CEO tells Senate,” CNBC, June 8, 2021, Accessed February 22, 2023, https://www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html.

62. Mark Gonloff, “Americans Are Now Hoarding Gas Instead of Toilet Paper,” Bloomberg, May 11, 2021, Accessed February 22, 2023, https://www.bloomberg.com/opinion/articles/2021-05-11/gas-shortage-panic-buying-makes-colonial-pipeline-hack-worse.; Christine Fernando, “Gasoline in plastic bags? Panic buying after Colonial Pipeline cyberattack won't solve the problem, experts say,” *USA Today*, May 12, 2021, Accessed February 22, 2023, https://www.usatoday.com/story/news/nation/2021/05/12/colonial-pipeline-cyberattack-anxiety-gasoline-panic-buying/5059184001/?gnt-cfr=1.

63. Falliere et al., *W32.Stuxnet Dossier*, 3.

64. Maria Henriquez, “Hacker breaks into Florida water treatment facility, changes chemical levels,” Security Magazine, February 9, 2021, Accessed February 22, 2023, https://www.securitymagazine.com/articles/94552-hacker-breaks-in-to-florida-water-treatment-facility-changes-chemical-levels.

65. Donald Stoker, *Why America Loses Wars, Limited War and US Strategy from the Korean War to the Present*, (Cambridge: Cambridge University Press, 2019), 22.

66. Thomas Rid, *Cyber War Will Not Take Place,* (Oxford: Oxford University Press, 2013), 1.

67. Aaron F. Brantly, "The Violence of Hacking: State Violence and Cyberspace," *Cyber Defense Review*, (Winter 2017): 73-91, Accessed February 22, 2023, https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/The%20Violence%20of%20Hacking_Brantly.pdf?ver=2018-07-31-093713-703, 76.

68. Brantly, "The Violence of Hacking: State Violence and Cyberspace," 77.

69. Singer and Friedman, Cybersecurity and Cyberwar, *What Everyone Needs to Know*, 124.

70. Singer and Friedman, Cybersecurity and Cyberwar, *What Everyone Needs to Know*, 124.

71. Singer and Friedman, Cybersecurity and Cyberwar, *What Everyone Needs to Know*, 88.