Title Page

# NotPetya: A Superlative Case of Cyber Strategy

Strategists Three

## Abstract

This essay is an examination of the NotPetya malware attacks perpetrated by Russian hackers against the country of Ukraine and a comparison of the methodology to the teachings of historical strategic analysists.  Additionally, books by Andy Greenberg, and David Sanger; and articles from WIRED, SecurityWeek, and the United States Department of Justice are examined for their insight into the events in Ukraine. The paper highlights the increasing utilization of cyber warfare in military strategy, its impact on civilians, and its replicant nature.

Keywords: NotPetya, Cyber Warfare, Ukraine, Russia, Military Strategy

# NotPetya: Cyber Warfare's Role in an Invasion

## Introduction

In the modern era, cyber warfare is inseparable from strategy. The world is interconnected, and actions taken by nations in regional conflicts can have immediate, and drastic, worldwide consequences. Such has been the case since Russia instigated an offensive, armed, and violent conflict with Ukraine in 2014 during a period of civil unrest in the former Soviet state. During this conflict Russia has been charged with perpetrating numerous cyberattacks against Ukraine, the most prominent being the NotPetya malware. The malware temporarily crippled companies and public infrastructure within Ukraine, eventually spreading across Europe and the world. However, Russia is not the only nation to incorporate cyber warfare in their strategy. As David E. Sanger, an author known for his contributions to national security, writes in *The Perfect Weapon,* the United States and Israel deployed a similar attack against Iranian nuclear production in 2012. NotPetya itself was built using hacks and exploits leaked from the United States of America's own National Security Agency (Graff, 2020). In *The Art of Warfare,* Sun-Tzu outlined the value of denying the enemy resources, of controlling and weakening the enemy while not engaging in combat, and of controlling logistics to influence the tide of war. Julian Corbett, in *Some Principles of Maritime Strategy,* expressed the strategic importance of securing resources and infrastructure from the enemy; these resources and infrastructure were the targets of the NotPetya attack. Corbett also provided guidance on influencing the populace to further the goals of the aggressor, and the methodical shutdown of civil life in Ukraine aligns with that stratagem. Andy Greenberg, a journalist who covers cybersecurity, wrote *Sandworm,* an entire book illustrating the damage done to everyday life in Ukraine due to one of the most devastating cyber-attacks in history.

These examples illustrate how NotPetya is the superlative demonstration of cyber warfare in strategy. Thus, the modularity, versatility, and widespread impact of cyber warfare make it an increasingly powerful and commonly implemented tool for both informing and executing strategy.

**The Presidential Suite**

Andy Greenberg interviewed the former president of Ukraine, Viktor Yushchenko, in 2017. Yushchenko declared that “Russia’s tactics, online and off have one single aim … to destabilize the situation in Ukraine, to make its government look incompetent and vulnerable” (Greenberg, 2019, p. 47). In the same interview, Yushchenko also said “Russia will never accept Ukraine being a sovereign and independent country,” followed by, “[in the last] twenty-five years since the soviet collapse, Russia is still sick with this imperialistic syndrome” (Greenberg, 2019, p. 47). Ukraine was part of Russia’s territory before gaining independence on August 24, 1991 and Russia views the conflict as though they are reclaiming lost territory. Therefore, it is inevitable that Russian attacks on Ukraine lead to cyberwarfare, for, while Clausewitz advised that

> [t]he first of these is *invasion*, that is *the seizure of enemy territory; not with the object of retaining it* but in order to exact financial contributions, or even to lay it waste. The immediate object here is neither to conquer the enemy country nor to destroy its army, but simply *to cause general damage*.
>
> (Clausewitz, 2008, p. 35, emphasis in original)

He also advises that “the original political objects can greatly alter during the course of [a] war and may finally change entirely *since they are influenced by events and their probable consequences*” (Clausewitz, 2008, p. 34, emphasis in original). Furthermore, according to

Greenberg, Ukraine is seen as a "scorched-earth testing ground for Russian cyberwar tactics" (Greenberg, Wired, 2018), and he later adds that "the Christmas blackout attack on Ukraine [in 2016] made [it] clear that Russia's hackers [are] indeed waging a cyber war" (Greenberg, 2019, p. 109).

It is also clear Russia harbors "economic jealousy [for Ukraine's position] as a lucrative pipeline route to Europe and its access to warm-water ports" (Greenberg, 2019, page 47). Thus, Yushchenko's warning that "[the] bell tolls for us all," that "[this] is a threat to every country in the world," (Greenberg, 2019, p. 48) is well worth heeding, and is further illustrated when Russia opportunistically annexed the Crimean Peninsula at the first sign of unrest in Ukraine. Russia may have acted shortsightedly in their annexation of Crimea, however. Machiavelli, in *The Prince*, posits that "in new Princedoms difficulties abound … it is essential that in entering a new Province you should have the good will of its inhabitants" (Machiavelli, 2005, p. 4). Russia also overlooks the advice that "limited war is only permanently possible to island Powers or between Powers which are separated by sea" (Corbett, 2018, p. 27). Without the good will of Ukraine's inhabitants and a with shared border with its enemy, Russia can expect continuing friction and the two nations now find themselves in the protracted Russo-Ukrainian War, with Russia searching for new ways to inflict damage upon Ukraine and further their political objectives.

Then, in August of 2016, reports surfaced of a large buildup of Russian military forces along the Ukrainian border line. Ukrainian forces, suspecting that this buildup was more than an attempt to "*keep the forces concentrated*" (Clausewitz, 1943, p. 148, emphasis in original), obliged the Russians and increased their presence in kind. Instead of a large-scale confrontation, however, the result of this standoff was a handful of foiled attempts at sabotage and some sporadic guerrilla engagements (BBC, 2016). A few months later, the war branched in a new direction and the first known successful cyberattack on a power grid, later attributed to the malware now known as Petya, was launched against Ukrainian infrastructure. The damage from the first attack was minimal, but it signaled a new means of engagement in warfare. Now military commanders have a new, indirect way to attack a state: via its infrastructure, its commerce, or even its public opinion. Perhaps, after two years, a means to end of the conflict was in sight, and,

> [s]ince the object of war is to force our will upon the enemy, the only way in which we can expect war on commerce to serve our end is to inflict so much damage upon it as will cause our enemy to prefer peace on our terms to a continuation of the struggle.
>
> (Corbett, 2018, p. 127)

The Russians seized these means, and other opportunities, to inflict such commercial damage upon Ukraine. What followed was a string of clandestine operations including the March 23, 2017 shooting of Russian government defector Denis Voronenkov on Ukrainian soil (Walker, 2017). Then, in April of the same year, the trojan for NotPetya was installed in M.E. Doc software (Cherepanov, 2017). Then, the Russians violent attempt to decapitate the Ukrainian military with the car bombing assassination of Colonel Maksym Shapoval (Luhn, 2017). Meanwhile, the authors of the NotPetya code had silently pushed their final updates and were waiting for day zero to execute (Cherepanov, 2017).

## Code Breaking

NotPetya surfaced on the eve of a Ukrainian public holiday: Constitution Day, June 27, 2017. NotPetya's damage is normally an estimation expressed in billions of dollars, but its actual effectiveness can be expressed by another metric: target saturation. At its height, 80% of computers infected with NotPetya were in Ukraine. If it were an immune system virus, like COVID-19, and Ukraine's computers were its people, it would have infected nearly 34 million Ukrainians in a matter of months using the same rate of reproduction. Analysis of the malware revealed that its "concealed intention" (Clausewitz, 1943, p. 146) was to destroy data (Kovacs, 2018), a clear indication that it was deployed to assist the attacker's goal of "cutting … communications … in such a way that the defender cannot re-establish them without considerable sacrifice" (Clausewitz, 1943, p. 538).

NotPetya's effects were felt across the whole country of Ukraine: the government, private companies, and civilians alike. The attack started in a small software company in Kyiv, the Linkos Group, the company responsible for handling M.E.Doc's accounting software fixes, so they were already integrated into the server forest (Greenberg, 2019, pp. 179-180). Initially, they were unaware of how badly compromised the servers were. Many individuals and companies who filed taxes in Ukraine were affected as a result of the compromised systems. Consequently, the whole nation was struck with the trauma and fear any natural catastrophe would inflict. Subsequently, Maersk, a global shipping line essential to Ukrainian infrastructure, Nuance, a speech recognition software that handles medical documents, and every company using M.E. Doc software around the world was affected. There was a total of $10 billion worth of infrastructure damages according to one White House assessment, though Greenberg (2019) emphasizes that to be just an approximate calculation (p. 199). Even international companies that have any connection with Ukraine were impacted, such as a chocolate factory in Tasmania, as well as every international docking terminal in the Maersk logistics chain.

The broader disruption of supply chains caused by the virus would mean that Ukraine would be unable to rely on their logistics which, as Sun-Tzu stated, is "the line between order and disorder" (Sun-Tzu, 1993, p. 120). These advantages would be hard-fought and well-needed for an attacker, as Ukraine is fighting on its homeland and defending its sovereignty. Sun-Tzu (1993) had recognized defense as the advantageous posture in a conflict, affording the defender the stronger position and necessitating that the attacker is certain that there is an advantageous opening before engaging (pp. 115-116). The defender, meanwhile, "reaps where he has not sown. Every intermission of the attack, either from erroneous views, from fear or from indolence, is in favor of the defender" (Clausewitz, 1943, p 317).

The widespread impact of the NotPetya attack illustrates the severity of cybersecurity vulnerabilities and highlights the distinct advantage exploiting a vulnerability may afford an attacker. Though the defensive side holds the stronger position, it can be weakened. Sun said that in defeating a defending enemy, "if [the enemy] cannot anticipate [the attack], the positions the enemy must prepare to defend will be many," and that "[to] be prepared everywhere is to be weak everywhere" (Sun-Tzu, 1993, p. 125). It is an impossible feat for Ukraine to harden every vulnerable system against exploitation. Even if it was known that such an attack was coming, the erratic nature of a worm and the vast amount of digital surface area to cover make it hugely expensive to secure every system. Once deployed, the NotPetya attack and its massive impact was effortless for the aggressors. This is a great advantage in war, and especially against a superior defense. According to Sun-Tzu, it is much preferred to "subdue the enemy's forces without going to battle, [to take] the enemy's walled cities without launching an attack, and [to crush] the enemy's state without a protracted war" (Sun, 1993, p. 111). Certainly, NotPetya provided a major blow to a state and demonstrated how malware, properly deployed, could turn the tide of a defensive war.

**The Sincerest Form of Flattery**

Four months later, in October of 2017, a new malware attributed to the authors of NotPetya was deployed against Ukrainian government computers. While this new version, called BadRabbit, was contained by disconnecting computers from the network, it still managed to infect over half of the Ukrainian government's computers (Greenberg, 2017). Then, unbeknownst to Olympic officials in China, another iteration, called Olympic Destroyer, was planted on their servers in November of 2017. Then the American government issued a warning in early 2018 "that Russian hackers had put 'implants' of malware in the nation's nuclear plants and power grid" (Sanger, 2018, p. xvi).

By the time Olympic Destroyer was implanted, the authors had taken great lengths to hide their identities and deflect responsibility for the cyberattacks. Nonetheless, they were eventually identified as the same hackers who authored NotPetya: a group known as Sandworm (Greenburg, 2019). Sandworm was first discovered by Drew Robinson, a malware analyst known as the "day walker" at the iSight intelligence firm. Robinson stumbled upon the username Arrakis02 from a malware code which was extracted from a PowerPoint presentation authored in Russia. Robinson says that these hackers might have been a huge fan of Frank Herbert's 1965 novel, *Dune*. "The [reason for the conclusion was] the word 'Arrakis' [which] is more than recognizable: it's [as] familiar as Tatooine or Middle-earth, the setting of a central pillar of the cultural canon. Arrakis is the desert planet" (Greenberg, 2019, p. 14), also known as Dune.

The realization that an entity, or entities, was quietly tunneling from host to host throughout the world at will drew a growing sense of concern from the international community. While Sandworm had spent years honing their skills punching holes through the networks of Ukraine like a canon shell through the hull of a battleship, other Russian hackers were using finer tools to unlock back doors for themselves halfway around the world. Their aim, it was later discovered, was to gather a trove of information from the upcoming 2016 American election (Sanger, 2018, pp. 205-209). While the whole threat actor group was later identified as belonging to the same branch of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU), it wasn't publicly acknowledged at the time because, among other reasons, the National Security Agency refused to sign off on the attribution (Sanger, 2018, p. 214).

Thus, while cyber warfare may inform strategy, it may also serve to misinform. While it may serve as a powerful weapon, it may also serve as a simple lever to pry open tightly secured boxes. Even as public opinion is still being shaped around cyberwar, actors are using their tools to influence the public. So, while those who control the cyber theater might prefer to operate unnoticed these, and other, malware attacks drew international attention to the vulnerabilities of an increasingly connected world. This culminates with the October 19, 2020 United States Department of Justice indictment filing which contends that "[t]hese GRU hackers and their co-conspirators engaged in computer intrusions and attacks intended to support Russian government efforts to undermine, retaliate against, or otherwise destabilize: (1) Ukraine; (2) Georgia; (3) elections in France; (4) efforts to hold Russia accountable for its use of a weapons-grade nerve agent, Novichok, on foreign soil; and (5) the 2018 PyeongChang Winter Olympic Games after Russian athletes were banned from participating under their nation's flag, as a consequence of Russian-government sponsored doping effort" (Office of Public Affairs, 2020).

## Conclusion

So, the former Soviet state of Ukraine remains hopeful they can regain control of their nation for, as Clausewitz said, "[h]owever small and weak a state may be in comparison with its enemy, if it forgoes a last supreme effort, we must say that there is no longer any soul left in it" (Clausewitz, 1943, pp. 461-462). The rest of the world must be vigilant and prepared because "NotPetya reminds us, [that] distance is no defense. Every barbarian is already at every gate. And [a] network of entanglements in that ether, [can] … bring [it] to a crashing halt" (Greenberg, 2017, p. 217). As such, other countries across the world have employed cyber warfare as instruments of strategy. The United States and Israel worked jointly on the StuxNet worm, deployed in Iran to disrupt their nuclear production. North Korea has been associated with a hack against Sony Pictures in America, in a supposed attempt to defend their leader's reputation. Russian hackers have been accused in meddling with elections in both Ukraine and the United States, going as far as allegedly hacking the Democratic National Convention and releasing their confidential documents, in an effort to sway the result of the vote. Cyber warfare can only be expected to grow as an implement of strategy; the great impact on targets and low consequence for perpetrators make it an invaluable tool. As the close examination of NotPetya demonstrates, malware can be deployed in many ways, which means nations must be prepared to protect themselves against forces lying in wait to inject their code into any advantageous vulnerability.

## References

British Broadcasting Corporation. (2016, August 12). *Ukrainian crisis: What's going on in Crimea?* BBC.com. https://www.bbc.com/news/world-europe-25182823

Cherepanov, A. (2017, July 4). Analysis of Telebot's Cunning Backdoor. *We live security*. https://www.welivesecurity.com/2017/07/04/analysis-of-telebots-cunning-backdoor/

Clausewitz, C. (1943). *On war* (O. J. M. Jolles, Trans.). Random House, Inc. (First published in 1832).

Clausewitz, C. (2008). *On war* (M. Howard & P. Paret, Trans., B. Heuser, Ed.). Oxford University Press. (First published in 1832)

Corbett, J. S. (2018). *Some principles of maritime strategy*. Adansonia Press. (First published in 1911).

Graff, G. M. (2020). *The man who speaks softly – and commands a big cyber army.* Wired. https://www.wired.com/story/general-paul-nakasone-cyber-command-nsa/

Greenberg, A. (2017, October 24). New ransomware linked to NotPetya Sweeps Russia and Ukraine. *Wired*. https://www.wired.com/story/badrabbit-ransomware-notpetya-russia-ukraine/

Greenberg, A. (2019). *Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers*. Anchor Books.

Greenberg, A. (2018, August 22). The untold story of NotPetya, the most devastating cyberattack in history. *Wired*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Greenburg, A. (2019, October 17). The untold story of the 2018 Olympics cyberattack, the most deceptive hack in history. *Wired. https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/*

Kovacs, E. (2018, February 16). U.S., Canada, Australia attribute NotPetya attack to Russia. *Security Week*. https://www.securityweek.com/us-canada-australia-attribute-notpetya-attack-russia

Luhn, A. (2017, June 27). *Ukrainian military intelligence officer killed by car bomb in Kiev*. The Guardian. https://www.theguardian.com/world/2017/jun/27/ukraine-colonel-maksim-shapoval-killed-car-bomb-kiev

Machiavelli, N. (2017). *The prince* (N. H. Tomson, Trans.). Ross Bolton. (First published in 1513).

Office of Public Affairs. (2020, October 19). *Six Russian GRU officers charged in connection with worldwide deployment of destructive malware and other disruptive actions in cyberspace*. The United States Department of Justice https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

Sanger, D. E. (2018). *The perfect weapon: War, sabotage, and fear in the cyber age.* Crown.

Sun-Tzu. (1993). *Sun Tzu: The art of warfare* (R. Ames, Trans.). Ballantine Books. (Original work published ca. 4th or 5th c BCE)

Walker, S. (2017, March 23). *Denis Voronenkov: Ex-Russian MP who fled to Ukraine killed in Kiev.* The Guardian. https://www.theguardian.com/world/2017/mar/23/former-russian-mp-denis-voronenkov-shot-dead-in-kiev