Why Do Offensive Cyber Operations Not Trigger Kinetic Military Responses?

Jake Sepich

SIS-795

Advised by Dr. Joshua Rovner

November 20, 2022

*For my parents and grandparents.*

*Without whose support, none of this would’ve been possible*.

**Abstract**

Why do offensive cyber operations (OCOs) not trigger kinetic military responses? This paper begins by exploring nuclear deterrence theory as the precursor to cyber deterrence. The analysis proceeds to first review research on the psychology behind OCOs. Next, this paper reviews the resilience of networks. Finally, the paper compares the differences between five forms of OCOs: cybercrime, disinformation, espionage, sabotage, and cyberwarfare. These comparisons include the severity of each form and the impact of attacks on various targets. The paper concludes by reviewing four cases that likely could have triggered a kinetic military response but didn’t do so. Two of these OCOs were attributed to Russian and two were attributed to China and Chinese-affiliated actors. This paper determines that to date cyber attacks have not been sufficiently severe to trigger a kinetic response because people view OCOs as being qualitatively different, networks are too resilient for significant damage to be done, and most undertaken forms of OCOs are simply not severe enough to trigger a kinetic response.

Introduction

 In 2022, the cost of a data breach reached an all-time high with a global average cost of $4.35 million.[[1]](#footnote-1) This is one example of the trend of both the costs to victims and frequency of offensive cyber operations (OCO) increasing in recent years. OCOs have targeted every aspect of society – from governments to private industry to individuals. These operations fit into a variety of categories, yet none of these have triggered a kinetic response. Some arguments claim that this is because actors can successfully deter adversaries from undertaking operations in cyberspace. This paper claims that an OCO has not triggered a kinetic military response because they are considered to be qualitatively different from kinetic military attacks, networks are durable and thus it is difficult to do permanent damage, and there are many forms of cyber attacks that can be more or less escalatory.

Literature Review

*Nuclear Deterrence*

Nuclear deterrence theory laid the groundwork from which cyber deterrence followed. Cyber deterrence has many differences but incorporated some important factors from previous waves of deterrence and thus these must be examined. While deterrence has its origins in the pre-modern age[[2]](#footnote-2), the theory came to prominence during the period following the end of World War II. Deterrence is defined as “the prevention of an adversary’s undesired action”.[[3]](#footnote-3) The opposite of deterrence is compellence, in which an actor makes another take a specified action. In both of these situations, the actor aims to ensure that the existing status quo is set up to support their goals. Combined, these make up the two aspects of coercive diplomacy. The common thread between both is the threat of violence if an actor’s demands are not followed.

William Kaufman establishes that three elements are required for deterrence: Cost, Capacity, and Intention. Costs in deterrence theory are the concept that an actor must undertake a “forecast about the costs and risks that will be run under certain conditions, and the advantages that will be gained if those conditions are avoided”.[[4]](#footnote-4) Deterrence succeeds when an adversary is convinced that the benefits that they would gain are outmatched by the costs that would be suffered as a result of taking a particular undesired action. Capacity is the concept that the “enemy must be persuaded not only that the instrument exists but also that its power is operational … [and] that it can get through to its targets and inflict a most burdensome cost upon him”.[[5]](#footnote-5) It is critical for an actor to ensure their adversary understands that they possess the capacity necessary to impose costs. If an adversary does not understand this, they may be willing to undertake larger risks with the belief that there will not be a response. Intention requires that an adversary must believe that an actor will follow through on using their capacity to impose costs. If the adversary does not believe this to be true, they will move forward with their preferred course of action. At this point, it is up to the actor to decide whether they will choose to move forward with their expressed threats. If they do not, an actor risks facing a loss of credibility and future adversaries potentially not taking their threats seriously.

There have been three main waves of nuclear deterrence, with scholars working to establish that a fourth wave is currently emerging.[[6]](#footnote-6) However, it is important to acknowledge that deterrence theory did not begin with the invention of nuclear weapons. Attempts to deter threats begin in antiquity, coming to prominence with the implementation of aircraft for military use at the turn of the 20th century. Before this, “bargaining [had] not really dealt with any popular suffering so great that the unique decision to fight or not to fight a war depended on an expectation of opponent’s restraint”.[[7]](#footnote-7) The shift came about because suddenly the considerations of war were not only the damage that one army could do to another; the risk of damage to both civilians and non-military infrastructure became a salient concern. Because of these new risks, each side would be concerned about its ability to maintain aircrafts to confront an attack from their adversary. International efforts were taken to mitigate these risks, such as the prohibition of dropping bombs from balloons at the Hague Conference in 1899.[[8]](#footnote-8) Despite these efforts, nations began to build various forms of aircrafts for military use.

These fears came to fruition with the bombings of civilian cities during WWII and reached their peak with the use of atomic bombs dropped from planes on Hiroshima and Nagasaki at the end of WWII. These bombings led to the first wave of nuclear deterrence as scholars wanted to avoid these weapons of mass destruction from ever being used again. However, the work during this period was perceived as being too far removed and too academic to be applicable at the time. While this wave was critical for beginning nuclear deterrence thinking, it did not have a significant long-term impact.

Deterrence theory came to prominence with the second wave, otherwise known as Rational Deterrence Theory. It is based on the assumption that a state's adversary is highly motivated to expand, the adversary understands that the state is defensive, and leaders on both sides are mainly concerned with the external, not domestic, situations.[[9]](#footnote-9) Theorists of this wave began to use game theory in their analysis, focusing on comparing deterrence to a game of chicken, where both actors will not back down until it is absolutely clear that one side can no longer gain the benefits that it hoped to achieve without withstanding an unacceptable level of costs. However, the importance of this wave was not so much in its theoretical implications, but in the work it did in becoming conventional wisdom among policymakers.

Despite becoming conventional wisdom, or perhaps because of it, many criticisms arose from Rational Deterrence Theory. One major concern was that this theory did not provide a solution for de-escalating situations; at best, it provided an outline of how to maintain an adverse relationship. Robert Jervis points out that in deterrence “mutual noncooperation is the worst outcome for both sides … [however] there are many important common interests between the sides.”[[10]](#footnote-10) This ties into the next criticism, that rational deterrence theory only works in high-conflict scenarios. Patrick Morgan examines this as one of his primary factors of deterrence. A third widely criticized aspect of second-wave deterrence was that it ignored the importance of rewards. Deterrence theory focused on the use of force and other negative responses while ignoring how benefits could provide adversaries with improved situations such that they would no longer need to follow through with undesirable actions. Finally, there was criticism that this theory overestimated the rationality of decision-makers. Some theorists, including Jervis, examined the decision making of policymakers and found that rationality did not hold in reality as they theorized it would.[[11]](#footnote-11)

The third wave of deterrence theory was a response to the issues inherent in the first two waves. Changes made throughout the third wave include the abovementioned topics to consider issues such as the impact of rewards, issues of misperception, and domestic and bureaucratic politics.[[12]](#footnote-12) There is an emerging fourth wave of deterrence theory that has been growing since the end of the Cold War with a primary focus on deterring asymmetric threats such as terrorist organizations. It was in this wave that cyber deterrence began to be considered in the larger concept of deterrence. Its largest divergence from previous waves is that the fourth wave no longer simply considers the relations between two sovereign states and now considers the possible impact of non-state actors, such as individuals or groups.

In his book “Deterrence Now”, Patrick Morgan described six key elements of deterrence theory: the assumption of a very severe conflict, the assumption of rationality, the concept of a retaliatory threat, the concept of unacceptable damage, the notion of credibility, and the notion of deterrence stability. The assumption of severe conflict operated on the basis that an adversary would attack if their enemy showed sufficient weakness such that an adversary state believed that an attack would be successful, and the adversary would not suffer significant losses. Because deterrence theory assumes that an actor will take advantage of any opportunity to attack, it did not consider alternative options for ending inter-state conflict, such as rewards. Deterrence theory also assumed that both sides would be rational. However, this prevented the theory from ever becoming fully satisfactory. People do not always act in ways that would provide them with greatest benefits immediately. Additionally, the importance that people put on taking actions now that will be beneficial to them at a later time varies depending on the action and are not consistent across all situations.[[13]](#footnote-13) Returning to Morgan’s elements, the notions of retaliatory threats and unacceptable damage are intertwined. States manipulate their opponent’s thinking by presenting the threat of unacceptable damage if the adversary does not do as they will. Any damage done by nuclear weapons would be unacceptable to a rational actor, meaning the threat of nuclear weapons should be able to deter attacks. Credibility in this situation relates to Kaufmann’s description of capacity. A state must not only have the capacity to impose costs, but its adversary must also believe that they have the capacity to impose an unacceptable level of costs. Finally, stability was a major problem during the Cold War. Both sides needed to maintain nuclear capacities that would balance the other, preventing all-out war. Sudden improvements in technology risked one side achieving the first-strike advantage and following through on the assumption of severe conflict.

Another aspect that Morgan discusses is the differentiation between general and immediate deterrence. General deterrence is conceived as occurring when an actor tries to deter a broad variety of actions or adversaries from considering these actions while immediate deterrence is undertaken in response to a threat that is already underway in an attempt to prevent it from coming to completion.[[14]](#footnote-14) The distinctions between these two forms are important for deterrence theory today; however, they were not often considered during the Cold War. The primary form of deterrence was general, with few instances of immediate deterrence, such as the Cuban Missile Crisis. These instances were few because of the danger each posed. Immediate deterrence during the Cold War risked creating situations that could lead to nuclear war while general deterrence focused on preventing actions that were undesired by the US such as the expansion of Communism.

Across all three waves, Herman Kahn identified two distinct forms of deterrence: Type I and Type II. Type I deterrence, or direct deterrence, focuses on attacks that are targeted against an actor’s homeland. Type II deterrence, or extended deterrence, focuses on deterring attacks against designated non-homeland targets. Extended deterrence requires making both allies and adversaries believe an actor will follow through with claims that they will defend external locations while direct deterrence is understood to be rational. Thomas Schelling proposed that belief in claims of extended deterrence could be achieved through brinksmanship.[[15]](#footnote-15) Extended deterrence is a frequent point of criticism in deterrence theory as it cannot be fully rational for a state to risk its safety for the security of another state.[[16]](#footnote-16) Because of this, states can threaten to reach a point where it would be easy to accidentally enter a war even if they would not actively choose to begin the war first. Additionally, extended deterrence was dependent on nuclear superiority.[[17]](#footnote-17) This is because the only way that extended deterrence could be credible and rational would be if a state could remove reciprocal threats. While extended deterrence remained a policy through the Cold War and beyond, there remain flaws in its fundamental logic.

 An important aspect when considering the implications of nuclear deterrence to future scenarios, including cyberspace, is the influence of the Cold War. Patrick Long establishes that the Cold War shaped what was assumed about deterrence.[[18]](#footnote-18) This is especially true regarding the fundamentally accepted principles such as severe conflict or deference to general deterrence in the literature. These concepts were developed during the period of the Cold War in conditions that have not been seen before or since. While the concepts may remain true, it is important to separate the conditions of the past from the present.

Two main strategies emerged from deterrence theory: deterrence-by-denial and deterrence-by-punishment. Deterrence-by-denial works by raising one’s defenses such that any attack by the adversary would not logically be able to succeed, removing the incentive to take undesired actions. Deterrence-by-punishment works by altering the cost/benefit analysis of an adversary through the threat of violence if they take an undesired action. Nuclear weapons provided the opportunity for credible deterrence-by-punishment. Before the creation of nuclear weapons, the possible damage threshold was not high enough to deter an adversary. It was most popular before the USSR had access to its nuclear weapons because, following their creation, the US could not credibly threaten nuclear punishment or a first-strike capability. Thus, both states transitioned to a second-strike capability which falls under the category of deterrence-by-denial. It is important to understand the difference between first- and second-strike capabilities to understand deterrence. First-strike capacity is an attack directed against the enemy’s means of retaliation.[[19]](#footnote-19) This attack would be considered successful if it destroyed all adversarial nuclear weapons or intercepted any which had been launched in response. Second-strike capacity is the ability to absorb an attack and retain nuclear weapons which can be used in response to the attack. The choice of a state to focus its strategy on either first- or second-strike capabilities changes how it interact with its adversaries.

Another key area of deterrence is the perception that policymakers utilize in deterrence scenarios. In “Deterrence and Perception”, Jervis focuses on the potential discrepancies in perception between a deterring state and its adversary. One of the most important claims of this paper is that the message a deterrer aims to send may not be the same message that an adversary receives. This comes from the fact that deterring states rarely considers the situation from its adversary’s perspective.[[20]](#footnote-20) Jervis’ argument can be distilled to the idea that deterrer’s are overconfident that their deterrence will succeed because they have not taken the proper time and energy to consider alternative perspectives which leads their adversaries to respond in unexpected ways.

Escalation is a phenomenon related to deterrence. Escalation is defined as the “[q]ualitative transformation in the character of a conflict in the direction of increasing scope and intensity.”[[21]](#footnote-21) During the Cold War, the two main thought leaders on the issue of escalation were Kahn and Schelling. Kahn believed that nuclear war could be controlled, and conventional war could be returned to following the use of a nuclear weapon. He recognized the importance of what came to be termed “firebreaks”[[22]](#footnote-22), which are psychological perceptions of a conflict moving from one level of severity to another but did not believe it was irrecoverable to return from the use of nuclear weapons. Schelling, on the other hand, believed it was best to never use nuclear weapons because their main strength was the perception of power, not their actual destructive power.[[23]](#footnote-23) He recognized the dangers of escalation and the fact that the actor who chose to begin escalating did not have the final say as to when escalation would be complete. That decision lay with the victim, not the attacker.

A variety of approaches evolved in the United States (US) during the Cold War for how to approach the strategy of deterrence policy. Massive retaliation was the first nuclear policy of the Cold War. On January 12, 1954, Secretary of State John Foster Dulles announced that American response to Communist efforts across the world would “depend primarily upon a great capacity to retaliate instantly by means and at places of our choosing”.[[24]](#footnote-24) The comments were understood to mean that the US would use nuclear weapons as tools of first response, but Dulles rebutted that idea in a later article for Foreign Affairs.[[25]](#footnote-25) In this piece, he claimed that the strategy did not aim to use nuclear weapons as the first means of response but it would not restrict the use of nuclear weapons under certain circumstances. However, this strategy was not sufficient because threats of massive retaliation could not be credible once the USSR had nuclear weapons as well. The US would not risk maximum retaliatory damage if they launched nuclear weapons. These considerations opened the idea of an appropriate response for actions below the threshold of nuclear launch.

Nuclear strategy changed significantly under President Eisenhower because the USSR gained nuclear weapons by the time of his election in 1952. His new policy, called the New Look, changed the focus from one of superiority to one of deterrence. However, this brought with it new challenges. The US could not provide credible extended deterrence once there was a risk of nuclear response from the USSR. While the first thought to make up the difference for these weapons was to use conventional forces, the concept of using tactical nuclear weapons soon emerged.

Tactical nuclear weapons are short-range weapons, including land-based missiles with a range of less than 500 km and air- and sea-launched weapons with a range of less than 600 km.[[26]](#footnote-26) These weapons would theoretically cause less damage than their counterparts in strategic nuclear weapons and defense strategists believed that they could use these weapons in battlefield scenarios without causing undue harm to surrounding civilian communities. These weapons were first researched by Project Vista, a program funded by the Army in the early 1950s. They found that tactical nuclear weapons could be useful in the defense of Europe[[27]](#footnote-27); however, some states did not want to sit in the middle of two warring nuclear states, especially considering that WWII had ended not long before. One major nuclear thinker who made his name around this concept was Henry Kissinger. His book “Nuclear Weapons and Foreign Policy” advocated for a flexible response strategy and disagreed with the strategy of massive retaliation.[[28]](#footnote-28) Flexible response moved away from the all-or-nothing nature of massive retaliation and provided more options for the US government to choose from. This in turn increased the credibility of its response by providing options that adversaries could be more likely to believe the US government would undertake.

Despite the theoretical popularity of tactical nuclear weapons, there were a variety of practical issues which interfered with their use. The first argument in favor was based on the concept that nuclear weapons would be a Western advantage over the USSR for a time to come.[[29]](#footnote-29) However, this was developed following WWII and the USSR quickly developed its first nuclear weapon by 1950. Their arsenal rapidly grew to a point that it would not be advantageous for the US to begin a nuclear confrontation. The second argument was that tactical nuclear weapons would favor defensive actors.[[30]](#footnote-30) This argument was opposed by military thinkers who pointed out that this relied on historical models of fighting where parties brought their entire forces together before attacking. This also relied on the attacking state failing to destroy their adversary’s nuclear weapons before attacking. The final argument, which had the greatest flaws, was the belief that tactical nuclear weapons would not do extreme damage to the surrounding communities.[[31]](#footnote-31) The argument claimed that these weapons could solely target military forces and leave civilians in peace and safety. However, it was discovered that radiation and force from nuclear weapons would spread too far to leave civilians unharmed. This concept was abandoned by the 1960s with Kissinger, its primary proponent, coming out in support of increasing conventional forces to make up for this loss.[[32]](#footnote-32)

Counterforce was a policy that RAND developed during the 1950s. This concept advocated for preemptive strikes in which the adversary’s nuclear weapons could be destroyed before launch. The main constraints on this policy were the quality of intelligence and the accuracy of missiles. A state using the counterforce policy needed a significant quantity of high-quality intelligence relating to its adversary’s nuclear weapon locations. This policy was not logically consistent if the state engaging in counterforce did not possess first-strike capabilities. It is challenging, if not impossible, to know where all adversary missiles are located. This is especially true with the advent of submarines that can launch nuclear weapons. Accuracy was the second point of contention with this policy. Counterforce specifically focused on attacking enemy military targets. It explicitly did not agree with the strategy of using nuclear weapons to attack civilian populations which was a crucial difference between it and mutually assured destruction. During the time of this strategy’s popularity, it was not feasible for the planned strikes to be accurate enough to guarantee not accidentally hitting civilian targets.

Secretary of Defense Robert McNamara based policies he undertook on the concept of mutually assured destruction, otherwise known as MAD. The idea behind this theory is that nuclear stability will be established through the risk of unacceptable damage which was quantified by the US government as 20-25% of civilian life lost and 50% of industrial capacity destroyed. [[33]](#footnote-33) No rational actor would begin a nuclear conflict if they understood the risks of a returning nuclear strike that was highly dangerous and not preventable. Despite policymakers officially supporting the theory of MAD, their actions did not support their words. President Nixon, in particular, attempted to avoid MAD. He originally attempted to upgrade the American nuclear force posture.[[34]](#footnote-34) This would have created a nuclear structure that was not balanced, as MAD would suggest, but instead strongly favored the US. Additionally, though his administration was responsible for negotiating both the SALT I and SALT II treaties, he was resistant to limiting anti-ballistic missile (ABM) systems and multiple independently targetable reentry vehicles (MIRVs).[[35]](#footnote-35) Despite being in a period of détente, which lasted from his presidency through the end of President Carter’s term, the US continued to take aggressive stances against the Soviet Union in an attempt to establish nuclear superiority that had not existed since the USSR developed nuclear weapons almost two decades before.

In addition to policymakers not acting in ways that the theory claimed they would, MAD faced opposition to its foundational ideas as well. Many opposed targeting civilian populations with nuclear weapons.[[36]](#footnote-36) Despite statements that nuclear launches need not necessarily target civilians, it would be impossible to avoid them with destruction at the scale advocated for by the theory. Critics went as far as to claim that MAD kept entire populations hostage. Tied to this is the disagreement in strategy from those who perceived MAD as an offensive strategy and wanted the US to instead focus on defending itself instead of attacking its enemies.[[37]](#footnote-37) Finally, this theory did not provide solutions for if deterrence failed, and nuclear war began besides using nuclear weapons to the point that a state’s adversary was decimated.[[38]](#footnote-38) Despite these criticisms, supporters consistently fell back on the fact that MAD has held so far, and peace has continued through a variety of situations that could have escalated to nuclear war.

An important concept that arose from the creation of MAD was the stability-instability paradox. Glenn Snyder proposed that MAD would deter nuclear war, but not conflict below the threshold of nuclear war and may encourage proxy conflict.[[39]](#footnote-39) The threat of nuclear weapons increases stability at that level of conflict but decreases stability at other levels. This paradox suggests that states would be comfortable confronting each other conventionally, but not at a nuclear level. However, states have often been hesitant to challenge each other directly even with purely conventional arms due to fears of escalation. This can be seen historically in Korea and Vietnam as well as currently in terms of American intervention in the 2022 Russian war versus Ukraine.

*Cyber Deterrence*

Before this paper can begin to address the concept of cyber deterrence in full, some terms must be defined. First, the term “cyberspace” is defined by the US government as “the interdependent network of information technology infrastructures … [that] includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers”.[[40]](#footnote-40) The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations is the result of a multi-year project where experts came together to create and release definitive guidance on cyber issues in the context of international law. This text defines a cyber attack as “a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects”.[[41]](#footnote-41) The manual also defines a cyber operation as an “operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful”.[[42]](#footnote-42) This paper will focus on cyber operations, specifically offensive cyber operations, because the inclusion of operations that do not reach the level of a cyber attack are critical to understanding cyber deterrence.

With these important definitions laid out, the concept of cyber operations can be traced back to the early 1990s at the beginning of what Stefan Soesanto and Max Smeets designated the “Early Period” of cyber deterrence work which lasted from 1990-2007.[[43]](#footnote-43) At this time, the US Department of Defense (DoD) focused on the concept of information warfare. Martin Libicki identified this concept as the belief that “[a]ll forms of struggle over control and dominance of information are considered essentially one struggle, and the techniques of information warfare are seen as aspects of a single discipline”.[[44]](#footnote-44) The first major public article about the issue came out of the Rand Corporation in 1993. John Arquilla and David Ronfeldt published a piece titled “Cyberwar is Coming!” in which they articulated their belief that “warfare is no longer primarily a function of who puts the most capital, labor, and technology on the battlefield, but of who has the best information about the battlefield”.[[45]](#footnote-45) They divided their concept of warfare into two separate and concrete proposals: netwar and cyberwar. Netwar is comparable to propaganda. The goal of netwar is to “disrupt, damage, or modify what a target population ‘knows’ or thinks it knows about itself and the world around it”.[[46]](#footnote-46) On the other hand, cyberwar refers to the use of information technology to augment kinetic force. In a cyberwar, one force would “[disrupt] if not [destroy] the information and communications systems, broadly defined to include even military culture, on which an adversary relies in order to ‘know’ itself’” before taking advantage of this information advantage to strike.[[47]](#footnote-47) This is similar to the beliefs of Sun Tzu who in his book *The Art of War* articulated “[s]o in war, the way is to avoid what is strong and to strike at what is weak”.[[48]](#footnote-48) If militaries chose to implement cyberwar, under Arquilla and Ronfeldt's definition, they would prevent adversaries from being able to communicate with each other before taking advantage of the chaos to strike.

Theories of cyber deterrence emerged from previous work on nuclear deterrence. However, the primary difference came in which form they focused on. While nuclear deterrence came to focus on deterrence by punishment, it was quickly realized that punishment would not work in the cyber realm. The issues of attribution, the credibility of response, and threats of escalation to physical violence meant that instead, the focus shifted to deterrence by denial. These issues became especially pertinent in 2007-2008 following Russian attacks on both Estonia and Georgia as actors realized that it would not be possible to engage in punishment against powerful actors without unacceptable consequences. This heralded the beginning of Smeets and Soesanto’s “Advancement Period” which lasted from 2007-2016.[[49]](#footnote-49) During this time many lines of thought became clarified. First, there emerged three primary meanings of cyber deterrence: military cyber deterrence to deter kinetic military attack, kinetic military means to deter a military cyber attack, and military cyber deterrence against other military cyber attacks.[[50]](#footnote-50) Additionally, scholars split into three distinct groups. The first recognizes that deterrence has fundamental problems, but the issues with cyber deterrence are not different from nuclear deterrence.[[51]](#footnote-51) Thus, it should succeed or fail as would be expected of nuclear deterrence. The second group rejects the concept that cyberspace is similar because cyberspace is different from the traditional domains of air, sea, air, and space.[[52]](#footnote-52) Thus, cyber deterrence must be considered differently. The final group does not believe cyber deterrence is possible.[[53]](#footnote-53) They believe that the attacker has such an advantage that cyber deterrence is an impossible goal.

While scholars debated the efficacy of cyber deterrence, Deputy Secretary of Defense William Lynn outlined a new cybersecurity strategy that was being undertaken by the US military in 2010. He emphasized the importance of protecting non-governmental networks and systems because of their importance to both internet infrastructure and the access that criminals can have.[[54]](#footnote-54) Despite this new focus, US government officials have been hesitant to use cyber weapons for offensive capabilities. This primarily has been due to the risk of escalation. In 2003, the Bush administration considered attacking Iraq’s financial system before beginning the invasion. However, this plan was scrapped over the fear of escalation and damage extending past Iraq to harm allies or the US itself.[[55]](#footnote-55)

Cyber deterrence within the US took a tangible turn in 2016, in a time termed the “Reflection Period” by Smeets and Soesanto.[[56]](#footnote-56) This shift was primarily due to Russian interference in the 2016 presidential election. Public attention on the issue skyrocketed and officials were forced to act. This was accompanied by the concept of defending forward in which the US would not wait for attacks but would instead work to prevent them before the attack could occur.[[57]](#footnote-57) Another important and related aspect was persistent engagement. Under this policy, the US would involve informing allies and partners regarding cyber threats and ideally working with them to eliminate these risks.[[58]](#footnote-58) While these threats exist, the abovementioned concepts fall under the umbrella of deterrence by denial because they aimed to limit the potential gains of adversaries through preemptive action.

 One aspect of cyber deterrence which has been focused on by experts is the issue of attribution. For many years, experts worried that governments would be unable to attribute attacks to the correct adversary, or, if they could, that it would take too long and lack the credibility to justify a response. However, this belief has been challenged by research by academic experts such as Thomas Rid, Ben Buchanan, and Jon Lindsay; industry professionals; and examples of successful government attribution. These efforts have been spearheaded by a small number of cybersecurity firms such as Mandiant, Crowdstrike, Recorded Future, and Microsoft. Academics have also come out with research that questioned previously held beliefs as industry professionals gained experience in attributing attacks and naming groups.[[59]](#footnote-59) Additionally, the US government has over time become more confident in naming attackers. The first major example was in 2014 when then-President Obama named North Korea as being responsible for the hack of Sony Pictures.[[60]](#footnote-60) This was a major event at the time and has led to subsequent willingness to take similar actions, such as believed threats to do so during Obama’s meeting with Xi Jinping after the Chinese hack of OPM, confronting Russia about the hack of SolarWinds, and naming China again for their hack of Microsoft Exchange. These have combined to show the possibilities of successfully attributing attacks. However, a major challenge remains in deterring OCOs. Credibility is the linchpin of deterrence[[61]](#footnote-61) and this requires rapid response after an attack has occurred. It is difficult to know if an attack in cyberspace is currently occurring and, even if an attack is known, it takes time to become certain regarding attribution. While the time required to be sufficiently confident of attribution has decreased, attackers may feel that the time between when an OCO begins, is discovered, and when the victim responds is long enough for them to achieve a goal and thus undertake the attack. Attribution in cyberspace will require not only decreased time between the attack and attribution to the adversary but also improved methods of detecting attacks to be meaningful in terms of deterrence.

Another issue in cyber deterrence is the offense-defense imbalance. This concept has been a base assumption of cybersecurity theory for as long as people have thought about the topic, going as far back as 1972.[[62]](#footnote-62) This concept focuses on the fact that an attacker must only find one gap in the defenses of their target while a defender must prevent every attack. With the rapid evolution of technology and frequent expansion of software to include new features, vulnerabilities in technologies are often not found before they are released to the public. In terms of deterrence, this means that attacking states have the advantage. This brings back the concept of second-strike capabilities. States must maintain their ability to respond, no matter the severity of an attack, to deter adversaries.

Analysis

*Perception of Cyber Attacks*

With these factors considered, the question remains: Why do OCOs not trigger kinetic military responses? The first reason is that people perceive OCOs in a different way than they perceive kinetic attacks. Research from Sarah Kreps and Jacquelyn Schneider supports this claim when they found that “individuals are far more reluctant to escalate in the cyber domain than for the corresponding conventional or nuclear attack. Indeed, the public exhibits far more caution when it comes to responding aggressively to cyber conflict than either conventional or nuclear”.[[63]](#footnote-63) Schneider undertook additional research at the Naval War College to examine this phenomenon. In her study, US government and military decisionmakers participated in war games and she focused on examining their willingness to use OCOs. She found that players cited concern about nuclear escalation to OCOs and faced psychological barriers to their use because “players created an equivalency between cyber and nuclear attack—any cyber attack would necessarily lead to a nuclear response”.[[64]](#footnote-64) In the only case where players chose to use OCOs, they did so as a preemptive attack. They perceived the risk of being attacked first and not being able to respond in kind as “so existential that they could not wait to respond to the cyber attack and therefore had to pre-emptively strike”.[[65]](#footnote-65) This shows how differences in risk perception change how willing a person is to undertake an OCO. This relates to additional research by Schneider and Julia Macdonald in which they examined presidential risk orientation and found that individual risk aversion, informed by both internal and external factors, shapes how willing a leader may be to take action in various domains.[[66]](#footnote-66) Schneider and Macdonald’s research showed that different decisionmakers vary in the level of risk that they are willing to accept across a variety of domains. Given that the wargames showed that decisionmakers are wary of escalation for fear of nuclear conflict, paricipants showed a high level of risk aversion. However, not every participant in those wargames avoided using OCOs. The level of risk that an individual decisionmaker is willing to accept, given that they have similar assumptions to participants of the wargames, affects their willingness to use OCOs. With this in mind, individuals with low-risk aversion would be significantly more likely to use OCOs than those with high-risk aversion. Kreps and Schneider also found that cyber operations are at the bottom of the escalation ladder because, for the public, cyberattacks are “qualitatively different than those of similar magnitude from other domains”.[[67]](#footnote-67) Given that this is true, the fact that decisionmakers are hesitant to use cyber operations in response to OCOs for fear of escalation means that it is unlikely that they would go further up the escalation ladder to undertake a kinetic attack.

Despite concerns of nuclear escalation, when participants were the victims of cyber attacks they determined that “cyber attacks were not worrisome enough to warrant a response”.[[68]](#footnote-68) A participant in the 2011 wargames stated that “cyber-attacks although annoying do not appear crippling”.[[69]](#footnote-69) This shows a high level of risk aversion but may come from an incorrect perception of the situation based on the facts. In “Deterrence and Perception”, Jervis discusses “self-deterrence” which is the concept that an actor can be deterred by figments of their imagination.[[70]](#footnote-70) This is to say, an actor may perceive their adversary as having more strength than they do or are more willing to escalate than they are. It appears that actors do not want to be the victims of OCOs but are unwilling to escalate, even within the cyber domain, because of concerns about racing up the escalation ladder to nuclear conflict. Despite these fears that an adversary would escalate to nuclear conflict, participants of the wargames did not find the attacks taken against them to be worrisome enough to justify escalation. Considering the misperception of decisionmaker and their risk aversion, Kreps and Schneider stated, “[i]f cyber represents a firebreak analogous to the difference between nuclear and conventional, then we would expect that actors would hesitate before escalating from the cyber domain to anything kinetic, whether conventional or nuclear irrespective of the nature of the hostile act”.[[71]](#footnote-71) This would explain why government officials have made statements like “[i]f you shut down our power grid, maybe we will put a missile down one of your smokestacks"[[72]](#footnote-72) yet there has been no kinetic response.

*Durability of Networks*

Another potential reason for escalation not occurring is that significant damage to networks is not possible because they are extremely durable. It is extremely difficult to do long-term damage to a network because it can be rebuilt and improved. Libicki, in his book *Cyberdeterrence and Cyberwar*, provides a convincing argument for network durability when he explains that “[a]s systems are attacked, vulnerabilities are revealed and repaired or routed around. As systems become more hardened, societies become less vulnerable and are likely to become more, rather than less, resistant to further coercion”.[[73]](#footnote-73) While networks are vulnerable to OCOs, these operations provide actors with an insight into their points of weakness. If the effects of an OCO can be mitigated, the victim of an attack can theoretically learn from their mistakes, make changes to strengthen their network, and mitigate future risks. This is closely tied to the concept of cyber resilience which the National Institute of Standards and Technology (NIST) defines as “[t]he ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources”.[[74]](#footnote-74) Resilience is important because it can be implemented to both take preemptive action against potential threats and to prepare policies for if an OCO has been successfully undertaken against a network. Because of this, US Cyber Command (USCYBERCOM) stated in their report “Achieve and Maintain Cyberspace Superiority” that “[the US can] sustain [its] strategic advantage by increasing resiliency, defending forward, and continuously engaging our adversaries”.[[75]](#footnote-75) Additionally, OCOs can be difficult to execute if actors undertake basic cyber hygiene. Most breaches occur against known vulnerabilities because it is difficult to create a zero-day exploit, which is a vulnerability in a system that the creator does not know about. As such, attackers frequently depend on systems not being updated, utilizing weak passwords, or social engineering. However, attackers face the risk of losing key assets which have been implanted to solutions as simple as their target updating a system and removing their entry point. Other forms of cyber hygiene, such as having strong passwords and regularly changing them as well as training employees on how to watch out for social engineering can reduce an actor’s risk surface area.

Not only can network security be improved and built up over time but it can also be quickly rebuilt if an OCO does cause significant damage. The best example of this comes from the leadup to Operation GLOWING SYMPHONY where USCYBERCOM took OCOs against the Islamic State of Iraq and the Levant (ISIS). Before this time, operations were undertaken to bring down ISIS servers, but they would come back up almost as soon as they could be taken down.[[76]](#footnote-76) This required an operation that attacked every server used by ISIS at the same time. This was only ten servers for this situation and USCYBERCOM was able to take down every server in use.[[77]](#footnote-77) For actors with less concentrated networks, this type of operation would not be possible. This is especially true for nation-states that have sprawling networks and have implemented redundancy to protect themselves from OCOs.

Finally, the increased use of cloud computing makes it more difficult for significant damage to be done to networks. An Amazon Web Services (AWS) cloud instance can be created in an average of under sixty seconds.[[78]](#footnote-78) Cloud services allow their clients to back up not only their data but also entire virtual machines (VM) and system configurations.[[79]](#footnote-79) These two factors allow actors to return to an operational state much more quickly in the aftermath of an attack. Additionally, a great deal of responsibility for infrastructure can be moved from the actor to the cloud service provider. While adversaries can exploit vulnerabilities in an actor’s implementation, the cloud service provider has an economic incentive to guarantee the safety, security, and upkeep of underlying cloud technology. Given that networks can be improved given that vulnerabilities are found, it is almost impossible to take down all of an actor’s vital networks, and cloud computing has reduced downtime, most OCOs are unable to do significant damage and are more annoying and economically harmful to victims than capable of causing substantial, long-term damage.

*Differences in Cyber Attacks*

Comprehending why there has not been a kinetic response to an OCO relies on understanding the differences between types of OCOs, their victims, and the targets of said attacks. This is critical because not all OCOs are the same and distinct types can be more or less escalatory. This paper will focus on five forms of OCOs – cybercrime, disinformation campaigns, espionage, sabotage, and cyberwarfare. While these are distinct categories, it is important to understand that operations overlap. This will be further discussed below.

Cybercrime is a set of actions or activities using a computer or network which violate the laws of at least one country. The perpetrators of these attacks can come either from within the said country or from a foreign nation. Some typical examples of cybercrime are torrenting movies, theft of money via phishing campaigns, and the use of ransomware. As this list shows, cybercrime is a very wide category that varies from mundane activities to extremely disruptive and costly operations. The issue with cybercrime is that, like all crime, it has historically been impossible to completely deter.[[80]](#footnote-80) There are too many actors who can reach the low threshold necessary to engage in cybercrime. Similar to physical crime, these threat actors must be mitigated, but they cannot be completely eradicated.

Disinformation campaigns require a higher level of coordination from the adversary. Disinformation is defined by the Department of Homeland Security as “false information that is deliberately spread with the intent to deceive or mislead”.[[81]](#footnote-81) While disinformation has always existed, its use has expanded with the invention of the internet and access to social media. Actors use algorithms’ in-group biases to circulate false information which confirms previously held beliefs. This has occurred through the use of targeted advertising, spreading memes, and blending in with other organizations that express similar views.[[82]](#footnote-82) These attacks have primarily come from groups that are either directly funded by or associated with foreign adversaries. This allows these groups to have access to the people and resources necessary to spread their messages. Major social media companies, such as Facebook and Twitter, have recently worked with US federal law enforcement organizations in an attempt to mitigate these campaigns, but it is unclear how successful they have been. Disinformation campaigns also take advantage of the gap between an OCO beginning and its attribution. While a disinformation campaign can be attributed and civilians warned of its occurrence, the adversary can begin to spread their message and cause harm before its detection.

Espionage affects all aspects of society. The Tallinn Manual defines cyber espionage as an “act undertaken clandestinely or under false pretenses that uses cyber capabilities to gather, or attempt to gather, information”.[[83]](#footnote-83) While espionage can target governments, it can also focus on trade secrets and private industry. In 2012, Director of the National Security Agency (NSA) Keith Alexander claimed that the loss of industrial information and intellectual property through cyber espionage constitutes the greatest transfer of wealth in history.[[84]](#footnote-84) China is responsible for vast quantities of theft of intellectual property. While this theft could also be classified as cybercrime, the theft of this information is often used to aid China’s larger strategic goals, such as catching up from technological disadvantages, rather than simply being sold for profit. Espionage can also be used to collect information on foreign assets, operations, or national secrets. An example of this came in 2008 when the Department of Defense was infected by malware which led to Operation Buckshot Yankee, which was responsible for clearing a worm that exfiltrated military data out of both classified and unclassified networks. While espionage can cause significant damage, there is an international norm that accepts the fact that states spy on each other. Although no state wants itself or its industries to have information stolen or be spied upon, espionage is accepted as a regular occurrence in both the physical and cyber realm. With that said, espionage may cause economic harm but is not intended to cause tangible damage to people or infrastructure.

Sabotage, on the other hand, is focused on causing tangible damage. The most famous example of cyber sabotage came from Stuxnet, otherwise known as Operation Olympic Games. This was an operation, attributed to the US and Israel, that targeted Iran with the aim of destroying nuclear centrifuges to delay the Iranian nuclear program. Cyber sabotage attacks aim to infect a target system and disrupt one or more functions necessary for them to continue operating. There have been significant worries about the possibility of an attack against critical infrastructure and key resources (CIKR) which could occur as attacking an electrical grid, water supply, or transportation systems as a few examples.

Cyber warfare, while conceptually worrying, has not yet occurred. Thomas Rid lays out a framework for what would define a cyberwar. For an OCO to be classified as warfare, it must be lethal, instrumental, and have a political nature.[[85]](#footnote-85) For an operation to be instrumental it must have a strategic purpose. The use of cyber tools must be intended for an action to result in a specific outcome. For it to be political, an OCO must aim to cause a clearly defined political outcome. Finally, an OCO must result in the death of individuals for it to be classified as warfare. While there have been examples of OCOs which have been instrumental and political, there has not been an OCO that has caused death.

Now that each type of OCO has been examined, it is important to recognize that there are firebreaks between each level of OCO. Cybercrime is generally considered to be petty and, like traditional crime, unable to be entirely prevented. It can also be difficult to attribute cybercrime, both because it may not be reported, but also because malware-as-a-service (MaaS) can obfuscate who is behind the attack given that a variety of people can use the same code while being unrelated to each other. There is generally minimal hesitancy to undertake cybercrime because of the lack of concern over being caught and the fact that cybercriminals from states such as Russia or China are unlikely to be punished unless they act against citizens of their own country. Moving up the escalation ladder, actors must be more coordinated and prepare for potential political fallout to undertake a disinformation campaign, due to both the level of resources required for successfully implementation and potential ramifications if the campaign is discovered. While disinformation campaigns are not inherently political, they are often undertaken to cause a political effect. Governments who are willing to sponsor these campaigns tacitly, if not openly, acknowledge the risks and blowback which may occur. However, blowback from a disinformation campaign would be less severe than if espionage was discovered. While it is known that states undertake espionage against each other, it remains a risk to both national integrity and intelligence secrecy. The occurrence of espionage is known, but its discovery worsens relations between states and can dissuade citizens from joining a state’s intelligence agencies for fear of being discovered working abroad. Additionally, adversary actors may discover methods of intelligence collection that had been secret upon the revelation of espionage. From this point, the severity of discovering espionage and the attribution of sabotage is the first firebreak between OCOs and has a significant risk of kinetic escalation. Sabotage does not always achieve its intended goal and it is up to the victim of sabotage to determine what they perceive to be an appropriate response. Actors who undertake sabotage must be willing to accept situations in which their operation does not achieve the desired goal and be ready to respond to any level of possible response. Finally, engaging in cyber warfare requires moving past another firebreak. It brings a campaign out of purely the cyber realm into the physical by causing the death of individuals. While sabotage can cause damage to infrastructure, the death of individuals results in the highest risk of escalation.

It is also important to understand the actors who can be responsible for these various OCOs. The four primary actors are nation-states, hacking groups, criminal organizations, and terrorist organizations.[[86]](#footnote-86) While there are both splinters and overlaps within and between these groups, these four are primarily responsible for most OCOs. Nation-states can be responsible for OCOs either by directing government agencies or their military to undertake the operation or by funding proxies to take actions. The number of nation-states that have both the technological capacity and available funds to do so is limited, and thus OCOs are highly concentrated among a few countries.[[87]](#footnote-87) China, Russia, and the US are all in the top five countries which OCOs come from.[[88]](#footnote-88) China has been estimated to have anywhere between 27-41% of the world's attacks coming from within its borders.[[89]](#footnote-89) While not all of these attacks are government-sanctioned, this statistic shows that a significant quantity of attacks come from a few countries, such as China, the US, Russia, North Korea, and Iran. Hacking groups can be independent cybercriminals, funded by a nation-state to act as proxies, or can be hacktivist groups that undertake cybercrime to pursue larger political, social, religious, or other ideological goals. While these groups are often incentivized by money, they do not have to be. Some criminal hacking groups produce MaaS but they may also directly use malware for attacks such as ransomware. Hacktivist groups will often act based on their purported morals. Groups such as Anonymous or patriotic hackers will undertake OCOs if they believe the victim is behaving in a way that justifies such an attack. There is significant overlap between hacking groups and criminal groups, especially in terms of groups who produce MaaS or who are funded to be proxies. Finally, terrorist groups are those who undertake kinetic terror activities and use the cyber domain to spread their message, extend the reach of the fear that they wish to cause, or fundraise. The prime example of a terror group that used OCOs is ISIS which used social media to widely spread its message, gain more followers for its cause, and fundraise from followers all around the world. While most of ISIS’ online operations were focused on propaganda and disinformation, some operations were undertaken to acquire information from governments that opposed its actions.[[90]](#footnote-90) Individuals may also lead OCOs, but they are not major actors; oftentimes, these individuals are in fact members of one of the larger groups mentioned above.

There are also important distinctions between those who are victims of OCOs. Great powers have a higher chance of escalation after suffering an attack than a regional or minor power. However, there may be a heightened chance that a lesser power will be attacked if they are a member of a security organization, such as NATO, or are under the protection of a great power such as Taiwan, Ukraine, or Belarus. Another important group of states to note are regional rivals who have cyber capabilities.

The greatest risk of kinetic escalation arises when a great power launches a cyber attack against another great power, especially when the OCO targets CIKR. These attacks risk the victim perceiving that the attacker is using an OCO as a preliminary action to weaken its target for a kinetic attack, thus triggering a retaliatory kinetic attack. This is what Jacquelyn Schneider calls the Capability-Vulnerability Paradox. She emphasizes that as states become more tied to digital technologies, there is an increased risk of a preemptive kinetic strike to prevent an adversary from destroying one’s digital infrastructure.[[91]](#footnote-91) While there are non-great powers with impressive cyber capabilities, none are as advanced as the modern great powers of Russia, China, and the US. As such, these three states face a heightened risk of their capabilities being undermined by an OCO. Additionally, OCOs from a lesser power may be seen as aggressive but are often unable to cause significant damage. Decisionmakers, as seen in Schneider’s war games, view OCOs as qualitatively different and are hesitant to move up the chain of firebreaks. If a great power does not believe that a state is imminently going to use an OCO to begin a larger-scale attack, as is the case with attacks that originate from lesser powers, said great power will not respond with kinetic force.

The existence of security organizations increases the odds of escalation for many states who would otherwise not be a risk for escalating in response to OCOs. The primary example of this is NATO, which is comprised of thirty member states across Europe as well as Turkey and the US. It was founded in 1949 to counter the Soviet Union and, after its collapse, has shifted to providing protection for its European partners from the new Russian Federation as well as working on other issues of international security. At the 2021 NATO Summit in Brussels, its members endorsed a new Comprehensive Cyber Defense Policy which states that “the impact of significant malicious cumulative cyber activities might, in certain circumstances, be considered as an armed attack”.[[92]](#footnote-92) This is a critical juncture from its previous position, which did not comment on the issue, because Article Five of the North Atlantic Treaty, which founded NATO, states that “an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and … [all Allies] will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force”.[[93]](#footnote-93) Although Article Five has only ever been invoked one time[[94]](#footnote-94), this decision raises the risk that a severe enough OCO against any member of NATO could justify its triggering again. This could cause a large-scale kinetic escalation against the responsible party. However, it is not just NATO for which this is the case. Other organizations which are involved in mutual security, such as the European Union, African Union, and Shanghai Cooperation Organization, face similar issues if they choose to come to similar conclusions regarding the issue of OCOs triggering kinetic responses.

There are also a variety of smaller states which are not involved in mutual security organizations that are either an ally of members in such security organizations or are provided significant security assistance by a great power. These states are significant for a variety of reasons, such as geographic location, political similarities, or historic alliances. Because of these reasons, great powers do not want these states to be taken over by geopolitical rivals, either by force or by political subterfuge, and may intervene in the case of a severe OCO. This raises the risk of kinetic escalation if either the protected state is unable to defend itself or if the opposing great power is concurrently attacked to prevent them from being able to assist their ally.

Lastly, it is important to acknowledge that while great powers are the primary risk points of escalation, there are a variety of highly advanced regional powers who are already in conflictual relationships and could be tempted to escalate in the face of an OCO. These flashpoints could occur in relations between Iran and Israel or North and South Korea, as a few examples. These states are in a consistent state of conflict and an OCO from either side could convince the victim that a kinetic attack is imminent and cause a preemptive strike in reaction. These states are at higher levels of risk not only because they frequently quarrel, but also because they have the capabilities to undertake OCOs which would be severe enough to cause significant damage to their adversary.

Finally, the target has an impact on the potential escalation in response to OCOs. As mentioned above, OCOs come in many forms. The response to an OCO cannot be one size fits all because the resulting damage significantly depends on what type of OCO was undertaken. It would not make sense for a state to react to cybercrime in the same way that it would react to cyber warfare. Cybercrime, disinformation campaigns, and espionage are not favorable for any state, but they are not actions that will likely trigger kinetic escalation. Cybercrime is similar to kinetic crime, and it has been found that the perception that one will be caught committing a crime is a more powerful deterrent than any form of punishment.[[95]](#footnote-95) Additionally, the damages done by cybercrime are significant when considered as a whole, but each attack does not do enough damage individually to warrant kinetic escalation. This does not negate the use of alternative solutions, such as indictments or attempting to work with the government of the state in which a criminal resides, but that is outside of the scope of this paper. Disinformation campaigns can result in significant societal harm, but they do not cause damages that would be justified in responding kinetically. These are actions that must be settled through a combination of domestic action to combat disinformation, diplomatic efforts to pressure states responsible for these campaigns to stop, and technical campaigns to take down servers where responsible individuals are working from. Finally, though not overtly, espionage is accepted and expected between states. Each state undertakes espionage, especially against their adversaries but also against allies, and as such, no state will likely escalate to kinetic force in response to an action that is accepted in international norms.

Sabotage and cyber warfare both risk targeting critical aspects of state security which could trigger a kinetic escalation. Sabotage can bring about some of the greatest risks that are considered when discussing cyber conflict. An actor could disrupt critical functions to sabotage an adversary’s CIKR such as the electric grid, nuclear command and control systems, or air traffic control systems. Actions at this level of damage may lead to kinetic escalation due to the harm that is done or the perceived risk of an imminent attack. None of these attacks have resulted in enough damage on their own to justify a kinetic response, but the risk of further attacks creates an environment in which a state may feel compelled to respond to protect itself. On other hand, it is likely that cyber warfare would immediately result in a kinetic response if it were to ever take place. Cyber warfare would not only have a political goal in mind, but it would also use lethal force to achieve that goal. Any state would be justified and compelled to kinetic action to protect their citizens from further attacks, punish the responsible actor, and dissuade other parties from considering similar actions in the future.

A final aspect to consider is if OCOs target the private sector compared to those focused on the public sector. The private sector has been at the forefront of cyberattacks because the largest technology companies and a massive amount of the underlying infrastructure is controlled by the private sector. However, the private sector does not have the capability to strike back against an individual, group, or state, regardless of the attack. These attacks are called hacking back and are outlawed in many countries. The private sector would need to convince the government of the country that they reside in that an attack is severe enough that undertaking a kinetic response is not only justified but also worth the material investment. This is not to say that it is impossible, or that the materials controlled by the private sector are not important enough to national security for a kinetic response to be justified, but it would be challenging for companies in many sectors to convince their governments to undertake these actions. Only attacks against CIKR sectors would likely be able to convince a state that a kinetic response is necessary. On the other hand, attacks against the private sector can be more damaging to national security. A state gaining access to key secrets, documents, or materials can severely set back a state’s national security strategy. However, this oftentimes is espionage, which has already been established has a norm that this is to be accepted at a certain level. Despite this, attacks against the private sector can focus on areas such as military intelligence, command and control (C2), or nuclear command, control, and communication (NC3). These attacks could be seen as precursors for a further kinetic advance by the attacking side. This form of OCO is inherently risky because the victim does not know what the next step will be and may choose to respond with force to defend themselves from being vulnerable to an unforeseen attack.

With all of these factors considered, it is clear that OCOs currently do not cause enough damage to trigger escalation to kinetic action. However, this does not mean that they do not have an effect on interstate relationships. OCOs can make diplomacy more difficult over time because they degrade trust between states. While cybercrime, disinformation campaigns, and espionage would not be severe enough to trigger kinetic escalation, it does not mean that any state wants to fall victim to any of these campaigns because they cause significant damage to the victim state and its citizens. Attribution becoming easier and more accurate means that victims have a higher chance of determining who was responsible for attacks in a timely manner. While states may have trouble holding non-state actors accountable, they may hold the state that those actors reside in responsible and request assistance in bringing the actor to justice. Additionally, if the responsible actor works directly for a state or is state-sponsored, the victim state will hold its adversary responsible for any actions taken. While this trade-off may be determined to be worth it for specific operations, it is important to acknowledge that this is an effect of these operations. More simply, we can say that OCOs affect a state’s grand strategy. Grand strategy is poorly defined but can be simplified as “an integrated scheme of interests, threats, resources, and policies. It is the conceptual framework that helps nations determine where they want to go and how they ought to get there.”[[96]](#footnote-96) OCOs can alter the state’s perception of who or what is a threat and how they should utilize policies and resources to combat this newfound threat.

One example of an altered grand strategy is the degraded diplomatic relationship between the US and Russia, especially since the Russian disinformation campaign targeted the 2016 US election. This interference, combined with a refusal to work against cybercrime coming out of its country, created a situation in which the US was not willing to tolerate future aggression by Russia. There is a stark comparison between the US reaction to the Russian invasion of Crimea in 2014 and its invasion of the rest of Ukraine in 2022. In 2014, the extent of the US reaction was messaging from the President’s office and the levy of sanctions against individuals deemed to be involved.[[97]](#footnote-97) In 2022, the US poured approximately $4.6 billion into Ukraine by June 1st, 2022, less than 100 days after the beginning of the invasion.[[98]](#footnote-98) Additionally, the US has not made efforts to find offramps that Russia would potentially find acceptable. In fact, the opposite has occurred, with President Biden continuing to send sending ever larger military shipments to Ukraine. The relationship between these two great powers has degraded since the Obama administration but the conflict has escalated since 2016. This is certainly in no small part due to the effects of Russian cyber operations against the US.

Case Studies

*Attacks Against Ukrainian CIKR from 2014-2017*

In the mid to late 2010s, Ukraine was affected by two OCOs against CIKR that were attributed to Russia. In December 2015, an OCO disrupted the Ukrainian electric grid and caused blackouts for over 225,000 customers.[[99]](#footnote-99) In 2017, Ukraine was affected by a pseudo-ransomware attack exploiting the EternalBlue and Mimikatz vulnerabilities which disrupted banks, hospitals, and government sectors.[[100]](#footnote-100) Both attacks were eventually attributed to Russia in its war against Ukraine which has been underway since it invaded Crimea in February 2014. Although both attacks were against Ukrainian CIKR, and Ukraine is an ally of the US in opposition to Russia, kinetic military escalation did not occur.

 From 2014 to 2016, a series of operations were aimed at Ukrainian CIKR, which were later attributed to Russia, specifically the Sandworm Team. The Sandworm Team is a threat actor who has been tied to Russia's General Staff Main Intelligence Directorate (GRU) Main Center for Special Technologies military unit 74455.[[101]](#footnote-101) They have been attributed with attacks targeting NATO countries, European governments, and industrial control systems (ICS).[[102]](#footnote-102) Attribution oftentimes comes from the use of BlackEnergy3, which has traditionally not been used to directly impact ICS, instead allowing attackers to remotely access systems to implant further malware which is used to accomplish this goal. BlackEnergy3 was found in all attacks against Ukrainian CIKR from 2014-2016.[[103]](#footnote-103)

These operations reached their peak in December 2015 when a cyber attack caused mass blackouts after an operation against three electric distribution companies when Russian actors used escalated privileges to open breakers in the Ukrainian power grid.[[104]](#footnote-104) After the incident occurred, an interagency team traveled from the US to Ukraine to aid in understanding the origins of the attack and work together to improve resilience in the Ukrainian power grid. During this time, the US provided aid to the Ukrainian government so that they could strengthen their power grid and other CIKR against future cyber attacks. Coordinated investigations found that BlackEnergy3 was delivered via malicious email attachments to employees of the impacted electric distribution companies.

Unfortunately, despite this aid from the US, Ukraine’s power grid was attacked by the Sandworm team yet again on June 27, 2017. This attack was dubbed NotPetya by Kaspersky Labs because it was a variant of the Petya ransomware.[[105]](#footnote-105) NotPetya is pseudo-ransomware, malware designed with the purpose of “[destroying] the victim’s systems rather than [offering] the opportunity to decrypt them”.[[106]](#footnote-106) The reason to use pseudo-ransomware instead of a wiper, which accomplishes the same task of destroying a system, is that it can hide the motivation behind an attack. Incident responders will see the immediate request for funds and assume it is traditional ransomware, only understanding that it is a wiper when it is too late to recover from the attack. This form of pseudo-ransomware does not provide the opportunity for attackers to decrypt a victim’s data, even if they do pay a ransom.[[107]](#footnote-107) This malware did spread across the world, but it is estimated that 60 percent of all systems affected by NotPetya were located in Ukraine. The campaign to launch NotPetya used two exploits: a modified version of EternalBlue[[108]](#footnote-108) and Mimikatz.

EternalBlue is an exploit developed by the NSA and leaked by a group called the Shadow Brokers that allows an attacker to “remotely execute arbitrary code and gain access to a network by sending specially crafted packets” in Windows systems.[[109]](#footnote-109) EternalBlue was combined with another exploit named Mimikatz which was created by a French researcher to prove that passwords on Windows systems, which are stored in a computer’s memory, could be pulled out of its Random Access Memory (RAM).[[110]](#footnote-110) These exploits were combined to allow actors behind the campaign to access the passwords necessary to spread and execute code that would restart a user’s computer and encrypt all data present on the system.[[111]](#footnote-111) While the original version of EternalBlue was patched by Microsoft, Mimikatz had not been and the ability to gain access to passwords allowed attackers to spread their reach across a variety of computers in a network. This malware was delivered to Ukrainian companies through software updates from the accounting software MeDoc, used by approximately 80% of Ukrainian businesses.[[112]](#footnote-112) These edited files were downloaded instead of the intended update and provided attackers with a backdoor, or an opening that a party knows about and can exploit to implant malware, as early as April 2017 before NotPetya was triggered at the end of June 2017.[[113]](#footnote-113)

However, despite being aimed at Ukrainian CIKR, NotPetya affected other companies and countries. A few examples were Maersk, Merck, and FedEx, and total damages cost more than $10 billion across all affected victims.[[114]](#footnote-114) For example, Merck had purchased insurance to protect against cyberattacks from a firm named Zurich. Once they were damaged by NotPetya, they filed a claim for $1.4 billion but this was rejected by Zurich, which claimed that the attack fell under the “war exclusion” clause in their policy to avoid payouts.[[115]](#footnote-115) This clause excludes insurance companies from needing to provide payouts for events that are acts of war. However, a New Jersey judge decided on January 13, 2022 that Zurich needed to pay this claim because the “language is meant to apply to armed conflict” and providers had not informed their clients that cyberattacks would not be covered.[[116]](#footnote-116) This decision does not clarify the current legal opinion on the status of cyberattacks as acts of war. It solely decided that this insurance provider had not provided adequate information to their client about what would or would not be covered and, as the contract stood, a cyberattack of this form would qualify to have claims paid.

It is important to understand why neither Ukraine nor the US chose to use kinetic military responses in reaction to these attacks. To begin with, Ukraine chose to utilize diplomatic denouncement instead of kinetic force. This is likely because Ukraine is not a major power. While they have the backing of the US, seeing that they did not receive support in 2014 to remove Russia from Crimea after its invasion, they likely believed that they would not receive the necessary support to begin an armed conflict. Additionally, Russia is a nuclear power and Ukraine is not. As has been seen during the 2022 Russia-Ukrainian war, President Putin has repeatedly expressed his willingness to use nuclear weapons to defend the Russian homeland. While the international community is currently defending Ukraine’s right to continue the conflict because of Russia’s aggression, it is unknown how states would have responded during that time if a situation began due to Ukraine responding militarily to a OCO. However, in the 2022 Russo-Ukrainian war, this situation may be different. Given the already existing kinetic conflict, Ukrainian allies would be more likely to support aggressive kinetic responses to similar attacks against CIKR. Despite the support that has been shown, Russia has attacked Ukrainian CIKR during this conflict, such as hacking satellite communications in March 2022[[117]](#footnote-117), yet Ukraine has not attacked the Russian homeland. This is likely because of the power discrepancy between these two states and a desire to avoid nuclear escalation.

For the US, leaders recognized the status of Russia as both another great power and a nuclear-armed state. Ukraine is a critical ally because of its geographic location, Western-leaning position, and democratic institutions. Despite these OCOs being the first of their kind against CIKR, they show the limitations of extended deterrence. According to the limitations of extended deterrence, the US would not be willing to risk damage to its own homeland to make a stand for Ukrainian security, especially when it risks escalation against another nuclear-armed state. Additionally, despite the damage done to the Ukrainian power grid, blackouts only lasted for six hours in 2015.[[118]](#footnote-118) This attack represented a significant shift as the first attack against CIKR, but it did not cause widespread, long-term damage to Ukrainian CIKR or major harm to its citizens.

*2016 Russian Election Interference*

Throughout the 2016 US election, Vladimir Putin directed various actors within the Russian government to undertake OCOs against the US to spread disinformation and undermine trust in the integrity of the U.S. presidential election.[[119]](#footnote-119) The Russian government hacked and subsequently leaked emails and documents from senior Democratic officials, used social media to spread disinformation, and ordered OCOs against election infrastructure. While not one of the 16 designated key infrastructure sectors in the US, election integrity is considered critical to a functioning democracy and the Russian interference caused significant political tensions. President Obama stated that “when any foreign government tries to impact the integrity of our elections ... we need to take action”.[[120]](#footnote-120) Despite this, in a similar fashion to the previous case, there was no kinetic reaction to an operation against a key aspect of American democratic society.

The Mueller investigation found that two units, FPN 26165 and FPN 74455 of the GRU, nicknamed Fancy Bear, carried out computer intrusions into Hillary Clinton’s presidential campaign, the Democratic National Committee (DNC), and the Democratic Congressional Campaign Committee (DCCC).[[121]](#footnote-121) These units implemented phishing campaigns to gain access to materials from employees and volunteers of the Clinton campaign, including high-level officials such as Clinton Campaign Chairman John Podesta.[[122]](#footnote-122) Phishing attacks are “counterfeit communications that appear to come from a trustworthy source but which can compromise all types of data sources”.[[123]](#footnote-123) These attacks are often used in espionage or cybercrime as the attacker uses a malicious email attachment, a false link, or other methods of delivering malware that is perceived as legitimate communications to gain access to a device to which they should not have access. Other forms of phishing can occur by spearphishing, a more targeted phishing scheme which targets high-level officials, such as the attack against John Podesta. Once an intruder has succeeded in their attack, they can use such privileges to gain access to sensitive files, such as emails or other documents, or they can move laterally across a network to gain access to more sensitive information. In this case, the successful spear phishing attack against Podesta resulted in the GRU stealing 50,000 of his emails.[[124]](#footnote-124)

The GRU also orchestrated spear phishing campaigns against the DNC and the DCCC. However, unlike the Clinton campaign, they continued to implant malware in both networks to exfiltrate documents from these organizations.[[125]](#footnote-125) This malware facilitated the capture and transfer of data from the DNC and DCCC to servers controlled by the GRU. From April - June 2016, the GRU exfiltrated approximately 70 gigabytes of documents and thousands of sensitive emails from the DNC and DCCC that were later released by WikiLeaks.[[126]](#footnote-126) Many of the materials were directly provided to WikiLeaks founder Julian Assange via Twitter by GRU agents using the pseudonym Guccifer 2.0 and from a Twitter account that appeared to originate within the US called DCLeaks.[[127]](#footnote-127) The US government and intelligence community have not established if Julian Assange knew that these individuals were Russian intelligence agents. The DNC emails were made available for public consumption on July 16, 2016,[[128]](#footnote-128) and emails from John Podesta were released on October 7, 2016.[[129]](#footnote-129) The release of Podesta’s emails, especially so close to the November 8 election day, resulted in an FBI-led investigation and the Obama administration's claim that Vladimir Putin was “engineering cyber-warfare breaches aimed at disrupting the democratic process and sowing doubt about the validity of the 2016 elections”.[[130]](#footnote-130) Despite later attribution from the US that these efforts originated from the Russian government, Russia has consistently denied involvement in any hack and leak operations. Following a Washington Post article that reported that Crowdstrike, the cybersecurity firm brought in by the DNC to remediate the breach, attributed the hack to Russia, the Kremlin spokesperson publicly claimed, “I completely rule out a possibility that the [Russian] government or the government bodies have been involved in this”.[[131]](#footnote-131)

At the same time as these operations were being undertaken by the GRU, the Internet Research Agency (IRA) led “overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or ‘trolls’”[[132]](#footnote-132) to manipulate American voters. This campaign used a variety of social media platforms, including Facebook, Instagram, Twitter, and YouTube.[[133]](#footnote-133) These accounts focused on pushing materials that both polarized the American political climate and were supportive of then-candidate Donald Trump.[[134]](#footnote-134) The material used targeted one of three groups: black Americans, left-leaning Americans, and right-leaning Americans.[[135]](#footnote-135) They coordinated this campaign by using networked output, which is an action that includes making a connection to some other user.[[136]](#footnote-136) They would target a user by becoming part of a group that they desired to influence. After connecting and creating an online rapport, the Russian account would begin to release content that was consistent with their target group’s biases. They would also use these connections to direct their connections to other accounts run by the IRA, which would then amplify their posts and share them to make it seem as if the post had originated with an American user. Despite this spread of Russian content, their accounts did not have massive followings. The domain with the highest number of impressions was blackmattersus.com which only had 1,327,862 impressions.[[137]](#footnote-137) The primary purpose of these accounts was not only to amplify the messages their own messages but also the messages of Americans who had the same beliefs that they were trying to spread. These posts were spread to others who held the same views and make them seem as if they were more mainstream than those beliefs actually were.[[138]](#footnote-138) While it was not the sole focus of this campaign to drive engagement to IRA accounts, the IRA’s efforts were successful in achieving higher-than-average levels of engagement with their posts. Engagement is defined by the clickthrough rate (CTR) of an advertisement or post. This is calculated by dividing the number of times a promoted post was clicked on by the number of times it was shown.[[139]](#footnote-139) On Facebook, the average CTR is .9%.[[140]](#footnote-140) This means that on average promoted materials on Facebook are clicked on by users to see more about the materials less than 1% of the time that anything is promoted. However, advertisements that were run by the IRA on Facebook exceeded the average CTR.[[141]](#footnote-141) These advertisements were able to have a greater impact on Facebook users than others that have been run through the platform, which shows the impact that the IRA was able to have through paid advertisement. Despite this higher level of engagement, the most that the IRA spent for one ad was only $1,649, which generated over 1.3 million impressions.[[142]](#footnote-142) Compared to traditional military influence operations, such as a $20 million operation run contracted by the US Special Operations Command during the “battle for hearts and minds” during the war in Iraq[[143]](#footnote-143), this operation was able to gain high levels of interaction for minimal investment.

Finally, the GRU attempted a variety of OCOs against US election infrastructure. The Senate Select Committee on Intelligence found that Russian-related actors targeted election infrastructure in at least eighteen states, and some actors in the intelligence community believe that number may have been as high as twenty-one states.[[144]](#footnote-144) While not all of these networks were breached, some states’ systems were scanned for issues as specific as voter registration information. Six states faced attacks against voting-related websites.[[145]](#footnote-145) In an unnamed small number of states, these actors were able to access restricted information and alter or delete voter registration information, though there is no evidence any changes were made.[[146]](#footnote-146) This reporting solely focuses on US state election infrastructure. It is unknown what level of attacks were targeted against political parties and other non-governmental organizations which participated in facilitating individual turnout and participation in the 2016 election.

Other attempts were made against companies critical to carrying out the 2016 election. The NSA examined one particular spear phishing campaign against a company that provided the sale of election-related software and hardware to states. The Russian actors used similar phishing techniques to those used in the previously mentioned campaigns. An email was sent to employees of the company with a Microsoft Word document that appeared to contain information about how an individual working for this company would properly configure election software onto a machine running Microsoft Windows.[[147]](#footnote-147) This document contained malware that would allow the actors to exfiltrate information and expand their privileges. The actors also attempted to mimic company email addresses in an attempt to sell election-related products and services to US-based targets on the state and local levels.[[148]](#footnote-148)

These operations fall under different categories: cybercrime, disinformation, and attempted sabotage respectively. Despite strong words from President Obama regarding the severity of these operations, not all of which were publicly known when he made his statements, there was no kinetic response to these operations. According to his statements, Russia was engineering cyber-warfare breaches. It is unclear why there was no kinetic military response by the US to what was called acts of cyber warfare, but there are a variety of potential answers. The first is that Hillary Clinton was the impacted party, a former member of Obama’s cabinet and a member of his party. As president, Obama may have wanted to seem impartial and not to further antagonize Russia for an event that was negatively impacting someone from his political party. However, if these operations were truly cyber warfare, as he claimed, then these actions should have surpassed party lines to justify a response that would protect future elections and guarantee that no party receives an advantage from foreign actors. As previously mentioned, not all facts about these OCOs were known during his time in office, which may have contributed to his course of action.

President Trump also chose to not respond kinetically during in his time despite the fact that both the Mueller Report and the Senate Select Committee on Intelligence’s report came out during his presidency and unequivocally attributed these campaigns to Russia. The only response of the Trump administration was to implement sanctions against the Russian government.[[149]](#footnote-149) This may have been because the election interference benefitted his campaign, and he did not feel the need to respond. There is no officially stated rationale for why the US has not responded militarily. However, this lack of response may have occurred because these operations, while a danger to the democratic integrity of the US, did not succeed in any larger-scale election corruption. There were risks to election infrastructure and Russia certainly worked to influence the opinions of citizens of the US, but it is not clear that these operations made a concrete difference in the 2016 election. These operations made the US more aware of its weaknesses and allowed adjustments to be made moving forward but were not considered sufficiently severe to trigger a response and risk escalation for operations that did not make a definitive difference in the election. This series of operations, while consequential for domestic politics, did not do sufficient tangible damage to justify a kinetic response. This came because of both the choices presidents during and after the operations combined with a lack of defined policy to dictate what would be the red line for appropriate escalation in the face of OCOs.

*APT-1*

Advanced Persistent Threat 1 (APT-1) is a cyber threat actor group located in China and is state-sponsored.[[150]](#footnote-150) Mandiant released a report in 2013 which exposed APT-1 of undertaking operations that stole “terabytes of data from at least 141 organizations” and 20 industries between 2006-2013.[[151]](#footnote-151) Security agencies have tracked them since this time, and they have been seen to be active as recently as 2018 but there have not been OCOs that have been publicly attributed to the group since that time.[[152]](#footnote-152) This group has allegedly stolen vast quantities of vital intellectual property (IP) from the US government and private industry. Despite this theft, which also can be classified as espionage, kinetic escalation has not occurred in an attempt to stem the tide of damages.

APT-1 is Mandiant’s designation for a group of Chinese actors associated with China’s People’s Liberation Army (PLA). Other organizations have different names for this group, such as CrowdStrike naming them PUTTER PANDA. Because it is believed that these groups significantly overlap, this paper will identify the group identified by both Mandiant and CrowdStrike in their respective reporting as APT-1. There is not complete overlap in the groups that are tracked by each company, but they have all tied these actors back to the 2nd Bureau of the PLA’s General Staff Department’s 3rd Department, otherwise known as PLA Unit 61398.[[153]](#footnote-153) Mandiant managed to track APT-1 to the exact same location in the Pudong New Area where the PLA’s 2nd Bureau operates, with 613 of 614 IP addresses that were used for exfiltrating information coming from only four blocks in Shanghai.[[154]](#footnote-154) Using this information, CrowdStrike was able to identify one of APT-1’s primary actors, a man named Chen Ping who goes by the alias cpyy.[[155]](#footnote-155) They were also able to tie APT-1 to a group they previously identified as working with Unit 61398 named COMMENT PANDA. This connection comes due to the common infrastructure used and evidence of communication between actors that are involved with both groups.[[156]](#footnote-156)

CrowdStrike identified APT-1 and COMMENT PANDA as targeting “[g]overnment, [d]efense, [r]esearch, and [t]echnology sectors in the US, with specific targeting of space, aerospace, and communications”.[[157]](#footnote-157) While Mandiant has identified actions that they have attributed to APT-1 outside of the US, they have observed 115 attacks against the US while the United Kingdom has been targeted with the second highest number at 5 attacks.[[158]](#footnote-158) This fact helps to explain why CrowdStrike’s reporting claims that APT-1 solely targets the US even though Mandiant has identified the group as being responsible for orchestrating attacks against targets abroad. These actors would periodically steal “broad categories of intellectual property, including technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, and emails and contact lists from victim organizations’ leadership”.[[159]](#footnote-159) APT-1 allegedly exfiltrated 6.5 terabytes of compressed data over a period of 10 months, the largest reported exfiltration event by the group reported by Mandiant.[[160]](#footnote-160) In addition, APT-1 breached the networks of more than 100 other companies but there is no event on record that matched the above-mentioned level of theft. However, not all industries have been affected equally. The information technology sector faced the earliest attacks, beginning in 2006, and was victim of the most compromises from 2006-2012 with attacks against almost 20 separate targets.[[161]](#footnote-161)

As a result of this theft, the Department of Justice (DOJ) indicted five members of PLA Unit 61398, believed to be members of APT-1, for “computer hacking, economic espionage and other offenses directed at six American victims in the U.S. nuclear power, metals and solar products industries” in 2014.[[162]](#footnote-162) In this indictment, the DOJ attributed these attacks to Unit 61398 due to a number of factors that have been outlined by Mandiant and CrowdStrike, in addition to the fact that most of the traffic occurred during traditional Chinese business hours which is a significant identifier towards this group originating in China.[[163]](#footnote-163) This was verified by research that had been undertaken by Mandiant, which was at that point owned by FireEye, but not yet released to the public.[[164]](#footnote-164)

APT-1 has a clear pattern that they follow when undertaking attacks:[[165]](#footnote-165)

* Initial reconnaissance: The group begins by scanning the networks of organizations that they are targeting for vulnerabilities to exploit. During this time, they may also research the structure of an organization, its hierarchy, and the personnel involved in different vital positions that would be susceptible to compromise. Some of these individuals include executives who can be targeted by spearphishing campaigns, human resources employees who could open infected email attachments, or assistants that can be targeted by social engineering.
* Initial compromise: This is the step that is traditionally considered hacking. At this point APT-1 uses one of many available tools, including those mentioned above, to gain access to the target network.
* Establish a Foothold: In this step, APT-1 works to prevent remediation of its breach upon discovery. One method of taking this step is creating innocuous user accounts. Another method involves implanting fileless malware, which is malware that can be difficult to discover because it is not written onto a disk.[[166]](#footnote-166) These steps cannot prevent the removal of access but aim to delay when this will occur.
* Escalation of Privileges: APT-1 uses this access to gain unauthorized privileges. Most often, an account is given administrator privileges so that it can make wide-sweeping changes to a network without needing to receive permission from another user. However, this step can also include providing lower levels of permissions, which are less obvious to those responsible for managing the network, if administrator privileges are not required to complete a mission.
* Internal reconnaissance: MITRE defines internal reconnaissance as the use of “malware or a similarly controlled application installed inside an organizational perimeter to gather information about the composition, configuration, and security mechanisms of a targeted application, system or network”.[[167]](#footnote-167) This is similar to the first step, initial reconnaissance; however, the difference between these two steps is that initial reconnaissance focuses primarily on how to gain entry to the network whereas internal reconnaissance focuses on gaining information that is not externally accessible.
* Move Laterally: After APT-1 has examined the points of weakness or interest, they begin to move from the original point of breach through the network. This both provides security against being removed from the systems through redundancy and allows them to gain access to new materials of interest.
* Maintain Presence: Once APT-1 has become established in a network, its main goal is to retain access, exfiltrate data, and determine where it can safely move within the network to gain further access without being discovered.

After these steps have been completed, APT-1’s actions depend on the scope of their campaign and the level of access they have been able to gain. If they do not wish to continue moving through the network, then they will either remove the malware to avoid attribution and move on to the next campaign or maintain the backdoor and move on if they believe that it will not be discovered. Otherwise, they restart this process at initial reconnaissance and continue until they have accomplished their goals, are discovered, or the exploit they have used is patched and their access is terminated.

(Figure 1)[[168]](#footnote-168)

Despite this massive loss of data, across a variety of sectors including government contractors, the US chose to implement a kinetic military response. The first potential reason is that China is a great power and President Obama engaged in a policy of “constructive cooperation”[[169]](#footnote-169) towards China. This may have led the Obama administration to believe that a positive relationship with China was more important than the loss of IP. Additionally, Cheng Li claims that “Obama and his team have refrained from pursuing paths that might lead to military confrontation”.[[170]](#footnote-170) A combination of then-President Obama’s belief in the potential for US-China cooperation and his desire to avoid military confrontation following the wars in Iraq and Afghanistan may have decreased his administration’s desire to engage in military conflict. Additionally, the Obama administration may not have believed that a kinetic military response would be the most effective method of response. President Obama and President Xi met in 2015 to discuss a variety of issues, one of which was cybercrime. In remarks after their discussions, President Obama announced that they had reached an agreement in which “neither the U.S. or the Chinese government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage”.[[171]](#footnote-171) To their credit, this agreement appeared to be successful. This agreement came in the wake of the US government developing a potential sanctions package against the Chinese government as a result of their passive support of cybercrime.[[172]](#footnote-172) In the year following this agreement, FireEye found that Chinese cybercrime breaches, many of which came from APT-1, dropped from 60 in 2015 to less than 10 by 2016.[[173]](#footnote-173) A final potential reason is that China is a nuclear-armed state. Despite the massive financial loss that the US government and industries faced as a result of the theft of IP, it is nowhere near the potential damages that would be incurred if a kinetic response escalated to nuclear conflict between these two great powers.

*OPM Hack*

In July 2014, the US government discovered that the personal files of 4.2 million former and current employees, as well as the security clearance information of 21.5 million individuals, had been exfiltrated to China in a coordinated operation by contractors hired by the Chinese government.[[174]](#footnote-174) Beginning in 2013, intruders breached the Office of Personnel Management’s (OPM) networks and began to lay the groundwork for a larger exfiltration campaign. This campaign continued for over a year with the intruders able to steal the “crown jewels” of US intelligence materials.[[175]](#footnote-175) Despite this titanic intelligence failure by the US, there was not a kinetic military response.

In the seven years prior to this breach, OPM had its cybersecurity rated as a “'material weakness’ because the agency had no IT policies or procedures that can come anywhere close to something that could be used as an excuse for securing the information”.[[176]](#footnote-176) This was despite their responsibility to maintain the security of background checks and security information for all US government employees. OPM’s issues were so severe that its Inspector General (IG) recommended temporarily shutting down computers that contained information regarding background investigations and security clearances because of potential national security implications.[[177]](#footnote-177) This idea was rejected because it would slow down the already arduous process of providing potential government employees with security clearances. The level of security was not improved during this time, even though OPM had been hacked five times in the previous three years.[[178]](#footnote-178) It was during this time that Chinese hackers first breached OPM. In this operation, they began to lay the groundwork for a larger attack by stealing manuals regarding OPM’s IT assets.[[179]](#footnote-179) This breach was not discovered for almost six months, during which time hackers breached two OPM contractors, the US Investigative Services (USIS) and KeyPoint, who were responsible for conducting investigations of potential US workers. The hackers were able to gain entry to USIS by compromising the credentials of employees.[[180]](#footnote-180) Despite its discovery, OPM chose to not publicly disclose the hack because it did not find that any personally identifiable information had been lost. Instead, they chose to implement a “big bang” system reset which theoretically removed the attackers from the system; however, this was undermined by a backdoor being implemented using credentials stolen from a KeyPoint employee.[[181]](#footnote-181) This backdoor was not discovered by OPM before the system reset, allowing the attackers to retain access to their systems. Despite this intrusion, OPM continued to not substantially improve its security systems. OPM failed to implement a variety of recommendations by its IG, including industry standards such as two-factor authentication.[[182]](#footnote-182) This allowed the actor which gained access to a KeyPoint employee’s username and password to freely access OPM’s networks. The reasoning for this choice given by OPM’s Chief Information Officer (CIO) at the time, Donne Seymour, was that “installing such gear in the government’s ‘antiquated environment’ was difficult and very time consuming”.[[183]](#footnote-183)

In addition to this lack of improvement of its own security system, OPM also was unable to properly review contractor system security. In May 2014, OPM reviewed the security systems of USIS, a contractor which was actively experiencing an unknown breach at the time, and did not raise any flags, instead giving them a rating of “met or exceeded the requirements imposed by government customers”.[[184]](#footnote-184) USIS informed OPM of the breach soon after but the breach had been underway for over six months at this time.[[185]](#footnote-185) Around the same time, the attackers began to exfiltrate both Standard Form 86 (SF-86) security clearance data and clearance adjudication information by breaching the Electronic Questionnaires for Investigative Processes (e-QIP) system.

SF-86 security clearance data contains a variety of information, including previous addresses, foreign travel, and information about an applicant’s personal life.[[186]](#footnote-186) However, there is additional information that clearance investigators gather that can be even more personal such as information about interviews with associated persons and record checks. This is all information that would not be available solely on the SF-86 form, but hackers were able to gain access to it by breaching OPM. Included in these additional materials was polygraph examination information. This is significantly more invasive than any of the previously breached data. In addition to these files, the hackers were also able to access the SF-85 form and the SF-85P questionnaire. The SF-85 form is used for non-sensitive government positions and the SF-85P questionnaire is used for individuals who work in “public trust positions”.[[187]](#footnote-187) A public trust position is one that does not work with materials that require a security clearance yet they “involve a significant degree of public trust and confidence that the Federal official will carry out the work in accordance with applicable laws, regulations and guidelines”.[[188]](#footnote-188)

It remains unclear if these databases were connected to Scattered Castles, the intelligence community’s (IC) community database of sensitive clearance holders.[[189]](#footnote-189) If this database was breached, it risks not only the knowledge of everyone who has a clearance being exposed to the Chinese government but also could have provided them with information about individuals who were disguised as State Department officers but are actually working for the IC or people from China who are providing information to the US.

These actors continued to exfiltrate data, including fingerprints of US government employees, as late as March 2015.[[190]](#footnote-190) It was discovered by individuals working within the defense sector, including the Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI), that this data was at risk in May 2015. After this discovery, the US Computer Emergency Readiness Team (US-CERT) worked with those agencies to begin investigating these intrusions. By using their intrusion detection system named Einstein, US-CERT found that Chinese actors breached a shared-service data center between OPM and the Department of Interior resulted in the personal data of 4.2 million federal employees being exfiltrated.[[191]](#footnote-191) Further investigations found that background investigation data had been exposed and exfiltrated.[[192]](#footnote-192) Finally, in June 2015, it was confirmed by OPM that security clearance information had been exfiltrated by Chinese actors.[[193]](#footnote-193)

Despite this massive loss of classified data, the US did not respond militarily to this breach. The first potential reason for this is that espionage is expected among states, especially between adversarial great powers. The US was upset that this breach occurred but most of the comments made questioned why OPM was so easily exploited and not why the Chinese exfiltrated this data. This norm of espionage, where states spy even on their allies but especially on their adversaries, meant that the US did not want to escalate to a kinetic military attack because it did not want to face the potential of a military response when it was caught conducting espionage in the future. Another reason is that China is an adversarial great power, and, like Schelling’s thinking on escalation, the US would not want to begin a conflict where it is unsure what level it would end at. The US could begin military escalation in response to a series of actions that are generally accepted on the international stage, but it would have no say on how the Chinese would respond and may feel their hand be forced to respond. However, this is not to say there was no response to the OPM hack. President Obama and Xi Jinping’s meeting in 2015 included discussions of OCOs. While their public statement focused on cooperation to counter cybercrime, it is reasonable to assume that the OPM hack was also discussed, as it could be classified as both espionage and cybercrime. Despite this agreement, nothing was said regarding the protection of governments against espionage. Additionally, the Department of Justice indicted and arrested an individual involved with this hack named Yu Pingan in 2017.[[194]](#footnote-194) Despite this diplomatic and law enforcement action and for the reasons stated above, there was no kinetic military response.

Conclusion

 This paper has aimed to answer why Offensive Cyber Operations (OCO) do not trigger kinetic military responses by providing various theories to answer this question and reviewing four cases that failed to escalate to kinetic military responses. The four cases – sabotage for the Ukraine case, disinformation for the 2016 election interference, cybercrime for APT-1, and espionage for the OPM hack – were selected to highlight four of the five identified forms of OCOs. There is no example of an OCO having all three of the qualities of cyberwarfare: being instrumental, having a political nature, and demonstrating lethality. It is thus unknown if an attack that contained all three of these qualities would trigger a kinetic military response, in contrast to all previous OCOs.

States must prepare for the growing possibility of kinetic military responses triggered by OCOs. There are already 2 major examples of states escalating conflict in response to OCOs: On August 24, 2015, the US killed Junaid Hussain, the mastermind behind ISIS’ cyber campaigns, including spreading disinformation, leading cybertheft campaigns, and encouraging supporters of ISIS to commit violent acts in their home nations.[[195]](#footnote-195) This drone strike occurred in the context of the larger US operation led by the FBI to eliminate individuals who he had radicalized within the US. On May 5, 2019, Israel responded to a still unspecified OCO from HamasCyberHQ.exe by launching an airstrike against a building containing Hamas operatives.[[196]](#footnote-196) This attack came during a time of heightened conflict between Israel and Palestine. While not the trigger of this conflict, Israel’s choice to use an airstrike against Hamas operatives was a clear point of escalation. These two events are similar in that both the US and Israel used kinetic military force as a decisive response to a perceived OCO in an active combat situation. Moreover, both military actions targeted leaders in adversary organizations who were using cyberspace to cause harm against aggressive actors targeting the respective states. These cyberattacks and accompanying military responses are likely to become the norm in the future of conflict because cyberspace has permeated every aspect of modern life. It is the foundation for not only military action but also the international finance system, government operations, and other critical services necessary for civilians. OCOs provide states with the ability to cause damage to their adversaries which was previously unconceivable, similar to the increase in damage that became possible when aircraft began being used by militaries. Because of the damage that OCOs can do to both military and civilian targets, those responsible for leading cyberspace operations will become increasingly high-priority targets, as generals who are responsible for the traditional domains of air, land, and sea have been historically.

States must also prepare for the increasing likelihood that future OCOs will cross the line to qualify as cyberwarfare. Though it may seem far-fetched at present, so did Stuxnet, the CIKR attacks in Ukraine, and the interference in the 2016 election. Due to the nature of escalation, the victim of this cyberattack can choose to escalate to a kinetic military response, and the attacker has little influence over the level of escalation. Moreover, states that have implemented policies such as NATO’s Comprehensive Cyber Defense Policy, decide that an OCO has finally exceeded their vague description of an attack that is severe enough to justify a kinetic response.

While there are many unknowns about why OCOs have not triggered kinetic military responses, it is clear that it is likely to happen in the future. OCOs exist in the rapidly changing cyber realm, and states are lagging behind private actors in their ability to make policy and keep up with the technological advancements. While OCOs have not yet triggered a kinetic military responses, it is likely that a future OCO will either be severe enough that a state is forced to escalate to a kinetic military response or a state will take advantage of an OCO to attack an adversary state, it is likely that this escalation will finally be seen.

Works Cited

Analyst Exchange Program, Combatting targeted disinformation campaigns: A whole-of-society issue § (2019).

Arquilla, John, and David Ronfeldt. “Cyberwar Is Coming!” *RAND Corporation*, 1993, 1–38.

Baig, Anas. “Top 5 Countries Where Cyber Attacks Originate.” Security Today, March 3, 2017. <https://securitytoday.com/articles/2017/03/03/top-5-countries-where-cyber-attacks-originate.aspx>.

Borghard, Erica D., and Jacquelyn Schneider. “Israel Responded to a Hamas Cyberattack with an Airstrike. That's Not Such a Big Deal.” The Washington Post. WP Company, May 10, 2019. <https://www.washingtonpost.com/politics/2019/05/09/israel-responded-hamas-cyberattack-with-an-airstrike-thats-big-deal/>.

Borys, Christian. “The Day a Mysterious Cyber-Attack Crippled Ukraine.” BBC Future. BBC, July 4, 2017. <https://www.bbc.com/future/article/20170704-the-day-a-mysterious-cyber-attack-crippled-ukraine>.

“CAPEC-529: Malware-Directed Internal Reconnaissance.” Common Attack Pattern Enumeration and Classification. MITRE, October 21, 2021. <https://capec.mitre.org/data/definitions/529.html>.

“Clickthrough Rate (CTR): Definition.” Google Ads Help. Google. Accessed November 17, 2022. <https://support.google.com/google-ads/answer/2615875?hl=en#:~:text=CTR%20is%20the%20number%20of,your%20CTR%20would%20be%205%25>.

“Collateral Damage: NotPetya Takes Russia's Cyber War Global.” GSI. S-RM Intelligence and Risk Consulting, August 1, 2017. <https://gsi.s-rminform.com/articles/collateral-damage-notpetya-takes-russias-cyber-war-global>.

“Compromise of a Power Grid in Eastern Ukraine.” Council on Foreign Relations. Accessed November 8, 2022. <https://www.cfr.org/cyber-operations/compromise-power-grid-eastern-ukraine>.

Computer Security Resource Center. “Cyber Resiliency - Glossary: CSRC.” CSRC Content Editor. NIST. Accessed October 15, 2022. <https://csrc.nist.gov/glossary/term/cyber_resiliency>.

Corera, Gordon. “Russia Hacked Ukrainian Satellite Communications, Officials Believe.” BBC News, March 25, 2022. <https://www.bbc.com/news/technology-60796079>.

Cox, Joseph. “The Malware That Led to the Ukrainian Blackout.” VICE, January 26, 2016. <https://www.vice.com/en/article/wnx5yz/the-malware-that-led-to-the-ukrainian-blackout>.

CrowdStrike Global Intelligence Team. Rep. *CrowdStrike Intelligence Report: Putter Panda*, 2016.

“Cyber Defence.” NATO, September 27, 2022. <https://www.nato.int/cps/en/natohq/topics_78170.htm>.

Cyware Labs. “APT1: A Nation-State Adversary Attacking a Broad Range of Corporations and Government Entities around the World: Research and Analysis.” Cyware Labs, June 6, 2019. <https://cyware.com/blog/apt1-a-nation-state-adversary-attacking-a-broad-range-of-corporations-and-government-entities-around-the-world-3041>.

Department of Homeland Security. “Fact Sheet: DHS Internal Working Group Protects Free Speech and Other Fundamental Rights When Addressing Disinformation That Threatens the Security of the US.” Fact Sheet: DHS Internal Working Group Protects Free Speech Other Fundamental Rights When Addressing Disinformation That Threatens the Security of the US | Homeland Security, May 2, 2022. <https://www.dhs.gov/news/2022/05/02/fact-sheet-dhs-internal-working-group-protects-free-speech-other-fundamental-rights#:~:text=The%20U.S.%20Department%20of%20Homeland,mislead%2C%20can%20take%20many%20forms>.

Detrow, Scott. “Obama on Russian Hacking: 'We Need to Take Action. and We Will'.” NPR. NPR, December 16, 2016. <https://www.npr.org/2016/12/15/505775550/obama-on-russian-hacking-we-need-to-take-action-and-we-will>.

DiResta, Renee, and John Perrino. “U.S. Influence Operations: The Military's Resurrected Digital Campaign for Hearts and Minds.” Lawfare. Brookings Institute, October 11, 2022. <https://www.lawfareblog.com/us-influence-operations-militarys-resurrected-digital-campaign-hearts-and-minds>.

Dulles, John Foster. “Policy for Security and Peace.” Foreign Affairs, April 1954. <https://www.foreignaffairs.com/articles/united-states/1954-04-01/policy-security-and-peace>.

Electronic Systems Division, and James P Anderson, Computer Security Technology Planning Study § (1972).

“Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements.” U.S. House of Representatives Permanent Select Committee on Intelligence. Accessed October 25, 2022. <https://intelligence.house.gov/social-media-content/>.

“Fact Sheet on U.S. Security Assistance to Ukraine.” U.S. Department of Defense, June 1, 2022. <https://www.defense.gov/News/Releases/Release/Article/3049483/fact-sheet-on-us-security-assistance-to-ukraine/>.

FireEye Labs. “The PLA and the 8:00am-5:00pm Work Day: FireEye Confirms DOJ's Findings on APT1 Intrusion Activity.” FireEye Blog, May 20, 2014. [https://web.archive.org/web/20140822053459/http://www.fireeye.com/blog/technical/2014/05/the-pla-and-the-800am-500pm-work-day-fireeye-confirms-dojs-findings-on-apt1-intrusion-activity.html](https://web.archive.org/web/20140822053459/http%3A//www.fireeye.com/blog/technical/2014/05/the-pla-and-the-800am-500pm-work-day-fireeye-confirms-dojs-findings-on-apt1-intrusion-activity.html).

Fruhlinger, Josh. “The OPM Hack Explained: Bad Security Practices Meet China's Captain America.” CSO Online. Foundry, February 12, 2020. <https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html>.

Global Research & Analysis Team. “Schroedinger's Pet(Ya).” SecureList. Kaspersky Labs, June 28, 2017. <https://securelist.com/schroedingers-petya/78870/>.

Gorman, Siobhan, and Julian E. Barnes. “Pentagon: Online Cyber Attacks Can Count as Acts of War.” The Wall Street Journal. Dow Jones & Company, May 31, 2011. <https://www.wsj.com/articles/SB10001424052702304563104576355623135782718>.

Gootman, Stephanie. “OPM Hack: The Most Dangerous Threat to the Federal Government Today.” *Journal of Applied Security Research* 11, no. 4 (2016): 517–25. <https://doi.org/10.1080/19361610.2016.1211876>.

Greenberg, Andy. “The Petya Plague Exposes the Threat of Evil Software Updates.” Wired, July 7, 2017. <https://www.wired.com/story/petya-plague-automatic-software-updates/>.

Greenberg, Andy. “The Untold Story of Notpetya, the Most Devastating Cyberattack in History.” Wired, August 22, 2018. <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>.

Green, Brendan. The Revolution That Failed: Nuclear Competition, Arms Control, and the Cold War. Cambridge: Cambridge University Press, 2020.

­­Hamid, Nafees. “The British Hacker Who Became the Islamic State’s Chief Terror Cybercoach: A Profile of Junaid Hussain.” *CTC Sentinel* 11, no. 4 (April 2018): 30–37.

IBM Security. *Cost of a Data Breach Report 2022*. Armonk, NY: IBM Corporation, 2022. Accessed November 16, 2022, <https://www.ibm.com/downloads/cas/3R8N1DZJ>.

Intelligence Community Personnel Security Database Scattered Castles § (2020).

Jasper, Scott. *Strategic Cyber Deterrence the Active Cyber Defense Option*. Lanham, MD: Rowman & Littlefield, 2017.

Jervis, Robert. “Deterrence and Perception.” International Security 7, no. 3 (1982): 3–30. <https://doi.org/10.2307/2538549>.

Jervis, Robert. “Deterrence Theory Revisited.” Edited by Alexander George and Richard Smoke. World Politics 31, no. 2 (1979): 289–324. <https://doi.org/10.2307/2009945>.

Jervis, Robert. “Rational Deterrence: Theory and Evidence.” *World Politics* 41, no. 2 (January 1989): 183–207. <https://doi.org/10.2307/2010407>.

Kaufmann, William W. *The Requirements of Deterrence*. Princeton, NJ: Center of International Studies, Princeton University, 1954.

Kissinger, H.A., and Dean, G. (1957). Nuclear Weapons and Foreign Policy (1st ed.). Routledge. <https://doi.org/10.4324/9780429046902>

Kreps, Sarah, and Jacquelyn Schneider. “Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving beyond Effects-Based Logics.” Journal of Cybersecurity 5, no. 1 (January 1, 2019): 1-11. <https://doi.org/10.1093/cybsec/tyz007>.

Lanfear, Terry. “Azure Backup and Restore Plan to Protect against Ransomware.” Azure backup and restore plan to protect against ransomware | Microsoft Learn. Microsoft, October 12, 2022. <https://learn.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware>.

Layne, Nathan. “U.S. Imposes Fresh Russia Sanctions for Election Meddling.” Reuters. Thomson Reuters, December 19, 2018. <https://www.reuters.com/article/us-usa-russia-sanctions-treasury/u-s-imposes-fresh-russia-sanctions-for-election-meddling-idUSKCN1OI27F>.

Li, Cheng. “Assessing U.S.-China Relations Under the Obama Administration.” Brookings, August 30, 2016. <https://www.brookings.edu/opinions/assessing-u-s-china-relations-under-the-obama-administration/>.

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND, 2009.

Libicki, Martin C. *What Is Information Warfare?* Washington, D.C.: Center for Advanced Concepts and Technology, Institute for National Strategic Studies, National Defense University, 1995.

Linvill, Darren L., and Patrick L. Warren. “Engaging with Others: How the IRA Coordinated Information Operation Made Friends.” Misinformation Review, July 26, 2022. <https://misinforeview.hks.harvard.edu/article/engaging-ira-coordinated-information-operation/>.

Long, Austin G. *Deterrence: From Cold War to Long War: Lessons from Six Decades of Rand Deterrence Research*. Santa Monica, CA: RAND Corp, 2008.

Lupovici, Amir. “The Emerging Fourth Wave of Deterrence Theory—Toward a New Research Agenda.” *International Studies Quarterly* 54, no. 3 (2010): 705–32.

Lynn III, William J. “Defending a New Domain.” Foreign Affairs, 2020. <https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain>.

Macdonald, Julia, and Jacquelyn Schneider. “Presidential Risk Orientation and Force Employment Decisions: The Case of Unmanned Weaponry.” *Journal of Conflict Resolution* 61, no. 3 (March 2017): 511–36. <https://doi.org/10.1177/0022002715590874>.

Main Intelligence Directorate Cyber Actors, [Redacted] Target U.S. Companies and Local U.S. Government Officials Using Voter Registration-Themed Emails, Spoof Election-Related Products and Services, Research Absentee Ballot Email Addresses; August to November 2016 § (n.d.).

Markoff, John, and Thom Shanker. “Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk.” The New York Times. The New York Times, August 1, 2009. <https://www.nytimes.com/2009/08/02/us/politics/02cyber.html>.

Morgan, Patrick M. *Deterrence Now*. Cambridge, United Kingdom: Cambridge University Press, 2003.

Mueller, Robert S., “Report on the Investigation into Russian Interference in the 2016 Presidential Election” § (2019).

Multi-State Information Sharing & Analysis Center. *Eternal Blue*.Washington, DC: US-CERT, 2019. <https://www.cisecurity.org/wp-content/uploads/2019/01/Security-Primer-EternalBlue.pdf>

Nakashima, Ellen. “Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say.” The Washington Post. WP Company, July 9, 2015. <https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/>.

Nakashima, Ellen. “U.S. Developing Sanctions Against China Over Cyberthefts.” The Washington Post. WP Company, August 30, 2015. <https://www.washingtonpost.com/world/national-security/administration-developing-sanctions-against-china-over-cyberespionage/2015/08/30/9b2910aa-480b-11e5-8ab4-c73967a143d3_story.html>.

Nakashima, Ellen. “Russian Government Hackers Penetrated DNC, Stole Opposition Research on Trump.” The Washington Post. WP Company, June 14, 2016. <https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html>.

Nakashima, Ellen, and Joby Warrick. “Stuxnet Was Work of U.S. and Israeli Experts, Officials Say.” The Washington Post. WP Company, June 2, 2012. <https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html>.

National Cybersecurity and Communications Integrity Center, IR-ALERT-H-16-043-01AP CYBER-ATTACK AGAINST UKRAINIAN CRITICAL INFRASTRUCTURE § (2016).

National Institute of Justice, "Five Things About Deterrence," June 5, 2016.
<https://nij.ojp.gov/topics/articles/five-things-about-deterrence>

NATO. “Collective Defence and Article 5.” NATO, September 5, 2022. <https://www.nato.int/cps/en/natohq/topics_110496.htm>.

New Knowledge, “The Tactics & Tropes of the Internet Research Agency”. Washington, DC: US Senate, 2019. Accessed November 4, 2018. <https://www.documentcloud.org/documents/5631777-Whitepaper-Final.html#document/p1>.

“New Petya / Notpetya / Expetr Ransomware Outbreak.” Kaspersky Daily. Kaspersky Labs, June 27, 2017. <https://usa.kaspersky.com/blog/new-ransomware-epidemics/11710/>.

Obama, Barack. “Remarks by President Obama and President XI of the People's Republic of China in Joint Press Conference.” The White House. National Archives and Records Administration, September 25, 2015. <https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint>.

Paret, Peter, Gordon A. Craig, and Felix Gilbert. 1986. Makers of Modern Strategy: From Machiavelli to the Nuclear Age. Princeton N.J: Princeton University Press.

Park, Donghui, and Michael Walstrom. “Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks.” The Henry M. Jackson School of International Studies. University of Washington, October 11, 2017. <https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/#_ftn2>.

Perlroth, Nicole. “In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back.” The New York Times. The New York Times, October 24, 2012. <https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?_r=0>.

Perlroth, Nicole, and Adam Goldman. “Chinese National Arrested in Connection with U.S. Cyberattacks.” The New York Times. The New York Times, August 25, 2017. <https://www.nytimes.com/2017/08/24/technology/chinese-national-arrested-cyberattacks.html>.

Quester, George H. *Deterrence before Hiroshima*. Routledge, 1986.

Rid, Thomas. “Cyber War Will Not Take Place.” *Journal of Strategic Studies* 35, no. 1 (2012): 5–32. <https://doi.org/10.1080/01402390.2011.608939>.

Rid, Thomas, and Ben Buchanan. “Attributing Cyber Attacks.” *Journal of Strategic Studies* 38, no. 1–2 (2015): 4–37.

Rogin, Josh. “NSA Chief: Cybercrime Constitutes the ‘Greatest Transfer of Wealth in History.’” Foreign Policy. Foreign Policy, July 9, 2012. <https://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/>.

“Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations.” U.S. Senate Select Committee on Intelligence, May 8, 2018. <https://www.intelligence.senate.gov/publications/russia-inquiry>.

Sanger, David E., and Nicole Perlroth. “U.S. Said to Find North Korea Ordered Cyberattack on Sony.” The New York Times. The New York Times, December 17, 2014. <https://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html>.

Sanger, David E., Julie Hirschfeld Davis, and Nicole Perlroth. “U.S. Was Warned of System Open to Cyberattacks.” The New York Times. The New York Times, June 5, 2015. <https://www.nytimes.com/2015/06/06/us/chinese-hackers-may-be-behind-anthem-premera-attacks.html?_r=0>.

Schelling, Thomas C and Anne-Marie Slaughter. *Arms and Influence*. Yale University Press, 2020.

Schmitt, Michael N. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. 2nd ed. Cambridge: Cambridge University Press, 2017.

Schneider, Jacquelyn. “Cyber and Crisis Escalation: Insights from Wargaming.” US Naval War College: 1-43.

Schneider, Jacquelyn. “Digitally-Enabled Warfare.” Center for a New American Security (en-US), August 26, 2019. <https://www.cnas.org/publications/reports/digitally-enabled-warfare-the-capability-vulnerability-paradox>.

Schneider, Jacquelyn G. “What War Games Tell Us About the Use of Cyber Weapons in a Crisis.” Council on Foreign Relations. Accessed March 14, 2022. <https://www.cfr.org/blog/what-war-games-tell-us-about-use-cyber-weapons-crisis>.

Senate, 5 Report of the Select Committee on Intelligence, US Senate, on Russian Active Measures, Campaigns and Interference in the 2016 U.S. election § (2020).

Segal, Adam. “The U.S.-China Cyber Espionage Deal One Year Later.” Council on Foreign Relations, September 28, 2016. <https://www.cfr.org/blog/us-china-cyber-espionage-deal-one-year-later>.

Smeets, Max. *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force*. Oxford University Press, 2022.

Snyder, Glenn H. *Deterrence and Defense: Toward a Theory of National Security*. Princeton, NJ: Princeton University Press, 1961.

Soesanto, Stefan, and Max Smeets. “Cyber Deterrence: The Past, Present, and Future.” In *NL ARMS Netherlands Annual Review of Military Studies 2020*, edited by Frans Osinga and Tim Sweijs, 385–400.

Soesanto, Stefan, and Max Smeets. “Cyber Deterrence: The Past, Present, and Future.” In NL ARMS Netherlands Annual Review of Military Studies 2020, edited by Frans Osinga and Tim Sweijs, 385–400. NL ARMS. The Hague: T.M.C. Asser Press, 2021. <https://doi.org/10.1007/978-94-6265-419-8_20>.

Sokov, Nikolai. “Tactical Nuclear Weapons (TNW).” The Nuclear Threat Initiative. James Martin Center for Nonproliferation Studies, April 30, 2002. <https://www.nti.org/analysis/articles/tactical-nuclear-weapons/>.

Stefanidis, Vasileios Angelos, Yiannis Verginadis, Daniel Bauer, Tomasz Przeździęk, and Gregoris Mentzas. (2020). Reconfiguration Penalty Calculation for Cross-Cloud Application Adaptations.

Temple-Raston, Dina. “How the U.S. Hacked Isis.” NPR. NPR, September 26, 2019. <https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis>.

Thrush, Glenn, and Annie Karni. “Podesta: Trump Ally Had 'Advance Warning' of Hacked Emails.” POLITICO, October 11, 2016. <https://www.politico.com/story/2016/10/podesta-fbi-investigating-email-hack-229648>.

Tzu, Sun. 2010. *The Art of War* (Chichester, England: Capstone Publishing).

“U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage.” The US Department of Justice, July 14, 2015. <https://www.justice.gov/usao-wdpa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and>.

USGS Human Capital Office. “Personnel Suitability Guidance Position Sensitivity and Public Trust Risk Level Determinations Q&A.” USGS. Accessed November 6, 2022. <https://www.usgs.gov/human-capital/personnel-suitability-guidance-position-sensitivity-and-public-trust-risk-level-0#:~:text=Q%3A%20What%20are%20public%20trust,applicable%20laws%2C%20regulations%20and%20guidelines>.

Vergun, David. “Leaders Discuss DOD's Cyber Strategy to Protect America, Partners.” U.S. Department of Defense, December 6, 2021. <https://www.defense.gov/News/News-Stories/Article/Article/2862784/leaders-discuss-dods-cyber-strategy-to-protect-america-partners/#:~:text=Defend%20forward%20also%20involves%20the,difficult%20to%20operate%2C%20he%20said>.

Vittorio, Andrea. “Merck’s $1.4 Billion Insurance Win Splits Cyber From ‘Act of War.’” Bloomberg Law, January 19, 2022. <https://www.bloomberglaw.com/bloomberglawnews/privacy-and-data-security/X1AQ4ER0000000?bna_news_filter=privacy-and-data-security#jcite>.

Warner, Matthew. “Wiperware (Pseudo Ransomware) Used in Ukraine Cyberattacks.” Security Magazine, March 2, 2022. <https://www.securitymagazine.com/articles/97176-wiperware-pseudo-ransomware-used-in-ukraine-cyberattacks>.

“What Is Fileless Malware?” CrowdStrike, March 22, 2022. <https://www.crowdstrike.com/cybersecurity-101/malware/fileless-malware/#:~:text=Memory%2Donly%20malware%20resides%20only,a%20foothold%20in%20an%20organization>.

WikiLeaks. “Search the DNC Email Database.” WikiLeaks, July 22, 2016, <https://wikileaks.org/dnc-emails/>.

WikiLeaks. “The Podesta Emails.” WikiLeaks, October 7, 2016. <https://wikileaks.org/podesta-emails/>.

1. IBM Security, *Cost of a Data Breach Report 2022*, (Armonk, NY: IBM Corporation), 5, accessed November 16, 2022, <https://www.ibm.com/downloads/cas/3R8N1DZJ>. [↑](#footnote-ref-1)
2. Austin G. Long. *From Cold War to Long War: Lessons from Six Decades of Rand Deterrence Research* (Santa Monica, CA: RAND Corp., 2008), 5. [↑](#footnote-ref-2)
3. US Department of Defense, *Joint Operational Planning*, Joint Publication 5-0 (Washington, DC: Office of the Chairman, Joint Chiefs of Staff, August 11, 2011): E-2. [↑](#footnote-ref-3)
4. William W. Kaufmann, *The Requirements of Deterrence* (Princeton, NJ: Center of International Studies, Princeton University, 1954), 12. [↑](#footnote-ref-4)
5. Ibid, 12-13. [↑](#footnote-ref-5)
6. Amir Lupovici. “The Emerging Fourth Wave of Deterrence Theory—Toward a New Research Agenda.” International Studies Quarterly 54, no. 3 (2010): 705–32. [↑](#footnote-ref-6)
7. George H. Quester. *Deterrence before Hiroshima* (Routledge, 1986), 2. [↑](#footnote-ref-7)
8. Ibid, 7. [↑](#footnote-ref-8)
9. Robert Jervis. “Rational Deterrence: Theory and Evidence.” World Politics 41, no. 2 (January 1989): 190. [↑](#footnote-ref-9)
10. Robert Jervis. “Deterrence Theory Revisited.” Edited by Alexander George and Richard Smoke. World Politics 31, no. 2 (1979): 294. [↑](#footnote-ref-10)
11. Robert Jervis. “Rational Deterrence: Theory and Evidence,” 203. [↑](#footnote-ref-11)
12. Amir Lupovici. “The Emerging Fourth Wave of Deterrence Theory—Toward a New Research Agenda”, 707. [↑](#footnote-ref-12)
13. Robert Jervis. “Rational Deterrence: Theory and Evidence,” 203. [↑](#footnote-ref-13)
14. Patrick M. Morgan, *Deterrence Now*, 9 [↑](#footnote-ref-14)
15. Thomas C. Schelling and Anne-Marie Slaughter. *Arms and Influence*, 99. [↑](#footnote-ref-15)
16. Robert Jervis. “Rational Deterrence: Theory and Evidence”, 186. [↑](#footnote-ref-16)
17. Austin G. Long, *From Cold War to Long War: Lessons from Six Decades of Rand Deterrence Research*, 22. [↑](#footnote-ref-17)
18. Ibid, 6. [↑](#footnote-ref-18)
19. Peter Paret et al., *Makers of Modern Strategy: From Machiavelli to the Nuclear Age* (Oxford: Clarendon, 1986), 753. [↑](#footnote-ref-19)
20. Robert Jervis. “Deterrence and Perception.” International Security 7, no. 3 (1982): 4. [↑](#footnote-ref-20)
21. Peter Paret et al., *Makers of Modern Strategy: From Machiavelli to the Nuclear Age*, 761. [↑](#footnote-ref-21)
22. Sarah Kreps and Jacquelyn Schneider. “Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving beyond Effects-Based Logics.” Journal of Cybersecurity 5, no. 1 (January 1, 2019): 2. [↑](#footnote-ref-22)
23. Peter Paret et al., *Makers of Modern Strategy: From Machiavelli to the Nuclear Age*, 761. [↑](#footnote-ref-23)
24. William W. Kaufmann, *The Requirements of Deterrence*, 3. [↑](#footnote-ref-24)
25. John Foster Dulles. “Policy for Security and Peace,” Foreign Affairs, April 1954, <https://www.foreignaffairs.com/articles/united-states/1954-04-01/policy-security-and-peace>. [↑](#footnote-ref-25)
26. Nikolai Sokov, “Tactical Nuclear Weapons (TNW),” The Nuclear Threat Initiative (James Martin Center for Nonproliferation Studies, April 30, 2002), <https://www.nti.org/analysis/articles/tactical-nuclear-weapons/>. [↑](#footnote-ref-26)
27. Austin G. Long, *From Cold War to Long War: Lessons from Six Decades of Rand Deterrence Research*, 44. [↑](#footnote-ref-27)
28. Henry A. Kissinger, Gordon Dean (1957). *Nuclear Weapons and Foreign Policy*, 282. [↑](#footnote-ref-28)
29. Peter Paret et al., *Makers of Modern Strategy: From Machiavelli to the Nuclear Age*, 746. [↑](#footnote-ref-29)
30. Ibid, 746. [↑](#footnote-ref-30)
31. Ibid, 746-747. [↑](#footnote-ref-31)
32. Ibid, 748. [↑](#footnote-ref-32)
33. Ibid, 758. [↑](#footnote-ref-33)
34. Brendan Green, *The Revolution That Failed: Nuclear Competition, Arms Control, and the Cold War*, 124. [↑](#footnote-ref-34)
35. Ibid, 125. [↑](#footnote-ref-35)
36. Peter Paret et al., *Makers of Modern Strategy: From Machiavelli to the Nuclear Age*, 758. [↑](#footnote-ref-36)
37. Ibid, 758. [↑](#footnote-ref-37)
38. Ibid, 758. [↑](#footnote-ref-38)
39. Glenn H. Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Princeton, NJ: Princeton University Press, 1961). [↑](#footnote-ref-39)
40. USG 50 USC § 1708 (d)(2) [↑](#footnote-ref-40)
41. Michael N. Schmitt. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), 415. [↑](#footnote-ref-41)
42. Ibid, 329. [↑](#footnote-ref-42)
43. Stefan Soesanto and Max Smeets, “Cyber Deterrence: The Past, Present, and Future.” In NL ARMS Netherlands Annual Review of Military Studies 2020, edited by Frans Osinga and Tim Sweijs, 385–400: 390 [↑](#footnote-ref-43)
44. Martin C. Libicki, *What Is Information Warfare?* (Washington, D.C.: Center for Advanced Concepts and Technology, Institute for National Strategic Studies, National Defense University, 1995), ix. [↑](#footnote-ref-44)
45. John Arquilla and David Ronfeldt, “Cyberwar Is Coming!”. *RAND Corporation*, 1993, pp. 1-38, 23. [↑](#footnote-ref-45)
46. Ibid, 28. [↑](#footnote-ref-46)
47. Ibid, 30. [↑](#footnote-ref-47)
48. Tzu, Sun. 2010. *The Art of War* (Chichester, England: Capstone Publishing), 23. [↑](#footnote-ref-48)
49. Stefan Soesanto and Max Smeets, “Cyber Deterrence: The Past, Present, and Future,” 390. [↑](#footnote-ref-49)
50. Ibid, 392. [↑](#footnote-ref-50)
51. Ibid, 392. [↑](#footnote-ref-51)
52. Ibid, 392. [↑](#footnote-ref-52)
53. Ibid, 394. [↑](#footnote-ref-53)
54. William J. Lynn III, “Defending a New Domain,” Foreign Affairs, 2020, <https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain>. [↑](#footnote-ref-54)
55. John Markoff and Thom Shanker, “Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk,” The New York Times (The New York Times, August 1, 2009), <https://www.nytimes.com/2009/08/02/us/politics/02cyber.html>. [↑](#footnote-ref-55)
56. Stefan Soesanto and Max Smeets, “Cyber Deterrence: The Past, Present, and Future,” 390. [↑](#footnote-ref-56)
57. David Vergun, “Leaders Discuss DOD's Cyber Strategy to Protect America, Partners,” U.S. Department of Defense, December 6, 2021, <https://www.defense.gov/News/News-Stories/Article/Article/2862784/leaders-discuss-dods-cyber-strategy-to-protect-america-partners/#:~:text=Defend%20forward%20also%20involves%20the,difficult%20to%20operate%2C%20he%20said>. [↑](#footnote-ref-57)
58. Ibid. [↑](#footnote-ref-58)
59. Thomas Rid, and Ben Buchanan. “Attributing Cyber Attacks.” Journal of Strategic Studies 38, no. 1–2 (2015): 4–37. [↑](#footnote-ref-59)
60. David E. Sanger and Nicole Perlroth, “U.S. Said to Find North Korea Ordered Cyberattack on Sony,” The New York Times (The New York Times, December 17, 2014), <https://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html>. [↑](#footnote-ref-60)
61. Austin G. Long, *From Cold War to Long War: Lessons from Six Decades of Rand Deterrence Research*, 11. [↑](#footnote-ref-61)
62. James P Anderson, “Computer Security Technology Planning Study,” Computer Security Technology Planning Study § (1972), pp. 1-33. [↑](#footnote-ref-62)
63. Sarah Kreps and Jacquelyn Schneider, “Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving beyond Effects-Based Logics”, 2. [↑](#footnote-ref-63)
64. Jacquelyn Schneider. “Cyber and Crisis Escalation: Insights from Wargaming.” US Naval War College, 20. [↑](#footnote-ref-64)
65. Ibid, 22. [↑](#footnote-ref-65)
66. Julia Macdonald and Jacquelyn Schneider. “Presidential Risk Orientation and Force Employment Decisions: The Case of Unmanned Weaponry.” Journal of Conflict Resolution 61, no. 3 (March 2017): 511–36. [↑](#footnote-ref-66)
67. Sarah Kreps and Jacquelyn Schneider. “Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving beyond Effects-Based Logics”, 8. [↑](#footnote-ref-67)
68. Schneider, Jacquelyn. “Cyber and Crisis Escalation: Insights from Wargaming”, 20. [↑](#footnote-ref-68)
69. Ibid, 20. [↑](#footnote-ref-69)
70. Robert Jervis, “Deterrence and Perception”, 14. [↑](#footnote-ref-70)
71. Sarah Kreps and Jacquelyn Schneider. “Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving beyond Effects-Based Logics”, 4. [↑](#footnote-ref-71)
72. Siobhan Gorman and Julian E. Barnes, “Pentagon: Online Cyber Attacks Can Count as Acts of War,” The Wall Street Journal (Dow Jones & Company, May 31, 2011), <https://www.wsj.com/articles/SB10001424052702304563104576355623135782718>. [↑](#footnote-ref-72)
73. Martin C. Libicki, “Cyberdeterrence and Cyberwar.” Santa Monica, CA: RAND, 2009: xv. [↑](#footnote-ref-73)
74. Computer Security Resource Center, “Cyber Resiliency - Glossary: CSRC,” CSRC Content Editor (NIST), accessed October 15, 2022, <https://csrc.nist.gov/glossary/term/cyber_resiliency>. [↑](#footnote-ref-74)
75. US Cyber Command, “Achieve and Maintain Cyberspace Superiority”, accessed October 15, 2022,

https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf, p. 6. [↑](#footnote-ref-75)
76. Dina Temple-Raston, “How the U.S. Hacked Isis,” NPR (NPR, September 26, 2019), <https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis>. [↑](#footnote-ref-76)
77. Ibid. [↑](#footnote-ref-77)
78. Vasileios Angelos Stefanidis, Yiannis Verginadis, Daniel Bauer, Tomasz Przeździęk, and Gregoris Mentzas. (2020). “Reconfiguration Penalty Calculation for Cross-Cloud Application Adaptations.” [↑](#footnote-ref-78)
79. Terry Lanfear, “Azure Backup and Restore Plan to Protect against Ransomware,” Azure backup and restore plan to protect against ransomware | Microsoft Learn (Microsoft, October 12, 2022), <https://learn.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware>. [↑](#footnote-ref-79)
80. Joseph S. Nye. “Deterrence and Dissuasion in Cyberspace.” International Security 41, no. 3 (January 2017): 45. [↑](#footnote-ref-80)
81. Department of Homeland Security, “Fact Sheet: DHS Internal Working Group Protects Free Speech and Other Fundamental Rights When Addressing Disinformation That Threatens the Security of the US,” Fact Sheet: DHS Internal Working Group Protects Free Speech Other Fundamental Rights When Addressing Disinformation That Threatens the Security of the US | Homeland Security, May 2, 2022, <https://www.dhs.gov/news/2022/05/02/fact-sheet-dhs-internal-working-group-protects-free-speech-other-fundamental-rights#:~:text=The%20U.S.%20Department%20of%20Homeland,mislead%2C%20can%20take%20many%20forms>. [↑](#footnote-ref-81)
82. New Knowledge, “The Tactics & Tropes of the Internet Research Agency” (Washington, DC: US Senate, 2019), 3-101: 34-50, <https://www.documentcloud.org/documents/5631777-Whitepaper-Final.html#document/p1>. [↑](#footnote-ref-82)
83. Michael N. Schmitt. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 168. [↑](#footnote-ref-83)
84. Josh Rogin, “NSA Chief: Cybercrime Constitutes the ‘Greatest Transfer of Wealth in History,’” Foreign Policy (Foreign Policy, July 9, 2012), <https://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/>. [↑](#footnote-ref-84)
85. Thomas Rid, “Cyber War Will Not Take Place,” *Journal of Strategic Studies* 35, no. 1 (2012): pp. 5-32, <https://doi.org/10.1080/01402390.2011.608939>, 7-8. [↑](#footnote-ref-85)
86. Scott Jasper, *Strategic Cyber Deterrence the Active Cyber Defense Option* (Lanham, MD: Rowman & Littlefield, 2017): 3. [↑](#footnote-ref-86)
87. Max Smeets, *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force* (Oxford University Press, 2022). [↑](#footnote-ref-87)
88. Anas Baig, “Top 5 Countries Where Cyber Attacks Originate,” Security Today, March 3, 2017, <https://securitytoday.com/articles/2017/03/03/top-5-countries-where-cyber-attacks-originate.aspx>. [↑](#footnote-ref-88)
89. Ibid. [↑](#footnote-ref-89)
90. Nafees Hamid, “The British Hacker Who Became the Islamic State’s Chief Terror Cybercoach: A Profile of Junaid Hussain,” *CTC Sentinel* 11, no. 4 (April 2018): pp. 30-37. [↑](#footnote-ref-90)
91. Jacquelyn Schneider, “Digitally-Enabled Warfare,” Center for a New American Security (en-US), August 26, 2019, <https://www.cnas.org/publications/reports/digitally-enabled-warfare-the-capability-vulnerability-paradox>. [↑](#footnote-ref-91)
92. “Cyber Defence,” NATO, September 27, 2022, <https://www.nato.int/cps/en/natohq/topics_78170.htm>. [↑](#footnote-ref-92)
93. North Atlantic Treaty Art. 5, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243. [↑](#footnote-ref-93)
94. NATO, “Collective Defence and Article 5,” NATO, September 5, 2022, <https://www.nato.int/cps/en/natohq/topics_110496.htm>. [↑](#footnote-ref-94)
95. National Institute of Justice, "Five Things About Deterrence," June 5, 2016, nij.ojp.gov:
<https://nij.ojp.gov/topics/articles/five-things-about-deterrence> [↑](#footnote-ref-95)
96. Rebecca Friedman Lissner, “What Is Grand Strategy? Sweeping a Conceptual Minefield,” *Texas National Security Review* 2, no. 1 (November 2018): pp. 52-73, 55-56. [↑](#footnote-ref-96)
97. “Executive Order 13660 of March 17, 2014, Blocking Property of Additional Persons Contributing to the Situation in Ukraine.” <https://obamawhitehouse.archives.gov/the-press-office/2014/03/17/executive-order-blocking-property-additional-persons-contributing-situat>. [↑](#footnote-ref-97)
98. “Fact Sheet on U.S. Security Assistance to Ukraine,” U.S. Department of Defense, June 1, 2022, <https://www.defense.gov/News/Releases/Release/Article/3049483/fact-sheet-on-us-security-assistance-to-ukraine/>. [↑](#footnote-ref-98)
99. “IR-ALERT-H-16-043-01AP CYBER-ATTACK AGAINST UKRAINIAN CRITICAL INFRASTRUCTURE ,” IR-ALERT-H-16-043-01AP CYBER-ATTACK AGAINST UKRAINIAN CRITICAL INFRASTRUCTURE § (2016), pp. 1-17: 1. [↑](#footnote-ref-99)
100. Christian Borys, “The Day a Mysterious Cyber-Attack Crippled Ukraine,” BBC Future (BBC, July 4, 2017), <https://www.bbc.com/future/article/20170704-the-day-a-mysterious-cyber-attack-crippled-ukraine>. [↑](#footnote-ref-100)
101. “Sandworm Team,” MITRE ATT&CK (MITRE), accessed November 18, 2022, <https://attack.mitre.org/groups/G0034/>. [↑](#footnote-ref-101)
102. Donghui Park and Michael Walstrom, “Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks,” The Henry M. Jackson School of International Studies (University of Washington, October 11, 2017), <https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/#_ftn2>. [↑](#footnote-ref-102)
103. Joseph Cox, “The Malware That Led to the Ukrainian Blackout,” VICE, January 26, 2016, <https://www.vice.com/en/article/wnx5yz/the-malware-that-led-to-the-ukrainian-blackout>. [↑](#footnote-ref-103)
104. “IR-ALERT-H-16-043-01AP CYBER-ATTACK AGAINST UKRAINIAN CRITICAL INFRASTRUCTURE,” 1-2. [↑](#footnote-ref-104)
105. “New Petya / Notpetya / Expetr Ransomware Outbreak,” Kaspersky Daily (Kaspersky Labs, June 27, 2017), <https://usa.kaspersky.com/blog/new-ransomware-epidemics/11710/>. [↑](#footnote-ref-105)
106. Matthew Warner, “Wiperware (Pseudo Ransomware) Used in Ukraine Cyberattacks,” Security Magazine, March 2, 2022, <https://www.securitymagazine.com/articles/97176-wiperware-pseudo-ransomware-used-in-ukraine-cyberattacks>. [↑](#footnote-ref-106)
107. Global Research & Analysis Team, “Schroedinger's Pet(Ya),” SecureList (Kaspersky Labs, June 28, 2017), <https://securelist.com/schroedingers-petya/78870/>. [↑](#footnote-ref-107)
108. “Collateral Damage: NotPetya Takes Russia's Cyber War Global,” GSI (S-RM Intelligence and Risk Consulting, August 1, 2017), <https://gsi.s-rminform.com/articles/collateral-damage-notpetya-takes-russias-cyber-war-global>. [↑](#footnote-ref-108)
109. Multi-State Information Sharing & Analysis Center. *Eternal Blue* (Washington, DC: US-CERT, 2019), <https://www.cisecurity.org/wp-content/uploads/2019/01/Security-Primer-EternalBlue.pdf> [↑](#footnote-ref-109)
110. Andy Greenberg, “The Untold Story of Notpetya, the Most Devastating Cyberattack in History,” Wired, August 22, 2018, <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>. [↑](#footnote-ref-110)
111. Global Research & Analysis Team, “Schroedinger's Pet(Ya)”. [↑](#footnote-ref-111)
112. Andy Greenberg, “The Petya Plague Exposes the Threat of Evil Software Updates,” Wired, July 7, 2017, <https://www.wired.com/story/petya-plague-automatic-software-updates/>. [↑](#footnote-ref-112)
113. Ibid. [↑](#footnote-ref-113)
114. Ibid. [↑](#footnote-ref-114)
115. Jennifer Roberts, “Summons to Appear: NotPetya and the War Exclusion Clause,” The SAIS Review of International Affairs (Johns Hopkins University, August 17, 2021), <https://saisreview.sais.jhu.edu/notpetya-and-the-war-exclusion-clause/>. [↑](#footnote-ref-115)
116. Andrea Vittorio, “Merck’s $1.4 Billion Insurance Win Splits Cyber From ‘Act of War,’” Bloomberg Law, January 19, 2022, <https://www.bloomberglaw.com/bloomberglawnews/privacy-and-data-security/X1AQ4ER0000000?bna_news_filter=privacy-and-data-security#jcite>. [↑](#footnote-ref-116)
117. Gordon Corera, “Russia Hacked Ukrainian Satellite Communications, Officials Believe,” BBC News, March 25, 2022, <https://www.bbc.com/news/technology-60796079>. [↑](#footnote-ref-117)
118. “Compromise of a Power Grid in Eastern Ukraine,” Council on Foreign Relations, accessed November 8, 2022, <https://www.cfr.org/cyber-operations/compromise-power-grid-eastern-ukraine>. [↑](#footnote-ref-118)
119. “Report of the Select Committee on Intelligence, US Senate, on Russian Active Measures, Campaigns and Interference in the 2016 U.S. Election,” 5 Report of the Select Committee on Intelligence, US Senate, on Russian Active Measures, Campaigns and Interference in the 2016 U.S. election § (2020), pp. 1-952, 7. [↑](#footnote-ref-119)
120. Scott Detrow, “Obama on Russian Hacking: 'We Need to Take Action. and We Will',” NPR (NPR, December 16, 2016), <https://www.npr.org/2016/12/15/505775550/obama-on-russian-hacking-we-need-to-take-action-and-we-will>. [↑](#footnote-ref-120)
121. Robert S. Mueller, “Report on the Investigation into Russian Interference in the 2016 Presidential Election,” Report on the Investigation into Russian Interference in the 2016 Presidential Election § (2019), pp. 1-182, 36. [↑](#footnote-ref-121)
122. Ibid, 38. [↑](#footnote-ref-122)
123. “What Is Phishing?,” Cisco (Cisco, July 28, 2022), <https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html>. [↑](#footnote-ref-123)
124. “Report of the Select Committee on Intelligence, US Senate, on Russian Active Measures, Campaigns and Interference in the 2016 U.S. Election”, 180. [↑](#footnote-ref-124)
125. Robert S. Mueller, “Report on the Investigation into Russian Interference in the 2016 Presidential Election”, 38. [↑](#footnote-ref-125)
126. Ibid 40-41 [↑](#footnote-ref-126)
127. Ibid, 46. [↑](#footnote-ref-127)
128. Julian Assange, “Search the DNC Email Database,” WikiLeaks, July 22, 2016, <https://wikileaks.org/dnc-emails/>. [↑](#footnote-ref-128)
129. Julian Assange, “The Podesta Emails,” WikiLeaks, October 7, 2016, <https://wikileaks.org/podesta-emails/>. [↑](#footnote-ref-129)
130. Glenn Thrush and Annie Karni, “Podesta: Trump Ally Had 'Advance Warning' of Hacked Emails,” POLITICO, October 11, 2016, <https://www.politico.com/story/2016/10/podesta-fbi-investigating-email-hack-229648>. [↑](#footnote-ref-130)
131. Ellen Nakashima, “Russian Government Hackers Penetrated DNC, Stole Opposition Research on Trump,” The Washington Post (WP Company, June 14, 2016), <https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html>. [↑](#footnote-ref-131)
132. “Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements,” U.S. House of Representatives Permanent Select Committee on Intelligence, accessed October 25, 2022, <https://intelligence.house.gov/social-media-content/>. [↑](#footnote-ref-132)
133. New Knowledge, “The Tactics & Tropes of the Internet Research Agency”, 7. [↑](#footnote-ref-133)
134. Ibid, 9-11. [↑](#footnote-ref-134)
135. Ibid, 12. [↑](#footnote-ref-135)
136. Darren L. Linvill and Patrick L. Warren, “Engaging with Others: How the IRA Coordinated Information Operation Made Friends,” Misinformation Review, July 26, 2022, <https://misinforeview.hks.harvard.edu/article/engaging-ira-coordinated-information-operation/>. [↑](#footnote-ref-136)
137. New Knowledge, “The Tactics & Tropes of the Internet Research Agency”, 34. [↑](#footnote-ref-137)
138. Darren L. Linvill and Patrick L. Warren, “Engaging with Others: How the IRA Coordinated Information Operation Made Friends”. [↑](#footnote-ref-138)
139. “Clickthrough Rate (CTR): Definition,” Google Ads Help (Google), accessed November 17, 2022, <https://support.google.com/google-ads/answer/2615875?hl=en#:~:text=CTR%20is%20the%20number%20of,your%20CTR%20would%20be%205%25>. [↑](#footnote-ref-139)
140. New Knowledge, “The Tactics & Tropes of the Internet Research Agency”, 37. [↑](#footnote-ref-140)
141. Ibid, 37 [↑](#footnote-ref-141)
142. Ibid, 38. [↑](#footnote-ref-142)
143. Renee DiResta and John Perrino, “U.S. Influence Operations: The Military's Resurrected Digital Campaign for Hearts and Minds,” Lawfare (Brookings Institute, October 11, 2022), <https://www.lawfareblog.com/us-influence-operations-militarys-resurrected-digital-campaign-hearts-and-minds>. [↑](#footnote-ref-143)
144. “Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations,” U.S. Senate Select Committee on Intelligence , May 8, 2018, <https://www.intelligence.senate.gov/publications/russia-inquiry>. [↑](#footnote-ref-144)
145. Ibid. [↑](#footnote-ref-145)
146. Ibid. [↑](#footnote-ref-146)
147. “Main Intelligence Directorate Cyber Actors, [Redacted] Target U.S. Companies and Local U.S. Government Officials Using Voter Registration-Themed Emails, Spoof Election-Related Products and Services, Research Absentee Ballot Email Addresses; August to November 2016,” Main Intelligence Directorate Cyber Actors, [Redacted] Target U.S. Companies and Local U.S. Government Officials Using Voter Registration-Themed Emails, Spoof Election-Related Products and Services, Research Absentee Ballot Email Addresses; August to November 2016 § (n.d.), pp. 1-5. [↑](#footnote-ref-147)
148. Ibid. [↑](#footnote-ref-148)
149. Nathan Layne, “U.S. Imposes Fresh Russia Sanctions for Election Meddling,” Reuters (Thomson Reuters, December 19, 2018), <https://www.reuters.com/article/us-usa-russia-sanctions-treasury/u-s-imposes-fresh-russia-sanctions-for-election-meddling-idUSKCN1OI27F>. [↑](#footnote-ref-149)
150. Mandiant, *APT1: Exposing One of China’s Cyber Espionage Units*, (Mandiant: 2013), 2, <https://www.mandiant.com/resources/apt1-exposing-one-of-chinas-cyber-espionage-units>. [↑](#footnote-ref-150)
151. Mandiant, *APT1: Exposing One of China’s Cyber Espionage Units, 3.* [↑](#footnote-ref-151)
152. Cyware Labs, “APT1: A Nation-State Adversary Attacking a Broad Range of Corporations and Government Entities around the World: Research and Analysis,” Cyware Labs, June 6, 2019, <https://cyware.com/blog/apt1-a-nation-state-adversary-attacking-a-broad-range-of-corporations-and-government-entities-around-the-world-3041>. [↑](#footnote-ref-152)
153. Mandiant. *APT1: Exposing One of China’s Cyber Espionage Units*, 2. [↑](#footnote-ref-153)
154. Ibid, 3-4. [↑](#footnote-ref-154)
155. CrowdStrike Global Intelligence Team, “CrowdStrike Intelligence Report: Putter Panda,” 2016, pp. 1-60, 5. [↑](#footnote-ref-155)
156. Ibid, 5. [↑](#footnote-ref-156)
157. Ibid, 5. [↑](#footnote-ref-157)
158. Mandiant. “APT1: Exposing One of China’s Cyber Espionage Units”, 22. [↑](#footnote-ref-158)
159. Ibid, 3. [↑](#footnote-ref-159)
160. Ibid, 25. [↑](#footnote-ref-160)
161. Ibid, 24. [↑](#footnote-ref-161)
162. “U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage,” The US Department of Justice, July 14, 2015, <https://www.justice.gov/usao-wdpa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and>. [↑](#footnote-ref-162)
163. Ibid. [↑](#footnote-ref-163)
164. FireEye Labs, “The PLA and the 8:00am-5:00pm Work Day: FireEye Confirms DOJ's Findings on APT1 Intrusion Activity,” FireEye Blog, May 20, 2014, [https://web.archive.org/web/20140822053459/http://www.fireeye.com/blog/technical/2014/05/the-pla-and-the-800am-500pm-work-day-fireeye-confirms-dojs-findings-on-apt1-intrusion-activity.html](https://web.archive.org/web/20140822053459/http%3A/www.fireeye.com/blog/technical/2014/05/the-pla-and-the-800am-500pm-work-day-fireeye-confirms-dojs-findings-on-apt1-intrusion-activity.html). [↑](#footnote-ref-164)
165. See Figure 1 [↑](#footnote-ref-165)
166. “What Is Fileless Malware?,” CrowdStrike, March 22, 2022, <https://www.crowdstrike.com/cybersecurity-101/malware/fileless-malware/#:~:text=Memory%2Donly%20malware%20resides%20only,a%20foothold%20in%20an%20organization>. [↑](#footnote-ref-166)
167. “CAPEC-529: Malware-Directed Internal Reconnaissance,” Common Attack Pattern Enumeration and Classification (MITRE, October 21, 2021), <https://capec.mitre.org/data/definitions/529.html>. [↑](#footnote-ref-167)
168. Mandiant, “APT1: Exposing One of China’s Cyber Espionage Units”, 27. [↑](#footnote-ref-168)
169. Cheng Li, “Assessing U.S.-China Relations Under the Obama Administration,” Brookings, August 30, 2016, <https://www.brookings.edu/opinions/assessing-u-s-china-relations-under-the-obama-administration/>. [↑](#footnote-ref-169)
170. Ibid. [↑](#footnote-ref-170)
171. Barack Obama, “Remarks by President Obama and President XI of the People's Republic of China in Joint Press Conference,” The White House (National Archives and Records Administration, September 25, 2015), <https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint>. [↑](#footnote-ref-171)
172. Ellen Nakashima, “U.S. Developing Sanctions Against China Over Cyberthefts,” The Washington Post (WP Company, August 30, 2015), <https://www.washingtonpost.com/world/national-security/administration-developing-sanctions-against-china-over-cyberespionage/2015/08/30/9b2910aa-480b-11e5-8ab4-c73967a143d3_story.html>. [↑](#footnote-ref-172)
173. Adam Segal, “The U.S.-China Cyber Espionage Deal One Year Later,” Council on Foreign Relations, September 28, 2016, <https://www.cfr.org/blog/us-china-cyber-espionage-deal-one-year-later>. [↑](#footnote-ref-173)
174. “The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation: Majority Staff Report,” The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation: Majority Staff Report § (2016), p. ii-231, v. [↑](#footnote-ref-174)
175. Ibid, iii. [↑](#footnote-ref-175)
176. “OPM: Data Breach,” OPM: Data breach: Hearing before the Committee on Oversight and Government Reform, House of Representatives, One Hundred Fourteenth congress, First Session § (2015), pp. 1-84, 2. [↑](#footnote-ref-176)
177. David E. Sanger, Julie Hirschfeld Davis, and Nicole Perlroth, “U.S. Was Warned of System Open to Cyberattacks,” The New York Times (The New York Times, June 5, 2015), <https://www.nytimes.com/2015/06/06/us/chinese-hackers-may-be-behind-anthem-premera-attacks.html?_r=0>. [↑](#footnote-ref-177)
178. “Under Attack: Federal Cybersecurity and the OPM Data Breach,” Under attack: Federal cybersecurity and the OPM Data Breach: Hearing before the Committee on Homeland Security and Governmental Affairs, US Senate, One Hundred Fourteenth congress, First Session June 25, 2015 § (2015). [↑](#footnote-ref-178)
179. Aliya Sternstein and Jack Moore, “Timeline: What We Know about the OPM Breach (Updated),” Nextgov.com (Nextgov, April 11, 2021), <https://www.nextgov.com/cybersecurity/2015/06/timeline-what-we-know-about-opm-breach/115603/>. [↑](#footnote-ref-179)
180. “Under Attack: Federal Cybersecurity and the OPM Data Breach”. [↑](#footnote-ref-180)
181. Josh Fruhlinger, “The OPM Hack Explained: Bad Security Practices Meet China's Captain America,” CSO Online (Foundry, February 12, 2020), <https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html>. [↑](#footnote-ref-181)
182. David E. Sanger, Julie Hirschfeld Davis, and Nicole Perlroth, “U.S. Was Warned of System Open to Cyberattacks”. [↑](#footnote-ref-182)
183. Ibid. [↑](#footnote-ref-183)
184. Aliya Sternstein and Jack Moore, “Timeline: What We Know about the OPM Breach (Updated)”. [↑](#footnote-ref-184)
185. Ibid. [↑](#footnote-ref-185)
186. Ellen Nakashima, “Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say,” The Washington Post (WP Company, July 9, 2015), <https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/>. [↑](#footnote-ref-186)
187. Gootman, Stephanie. “OPM Hack: The Most Dangerous Threat to the Federal Government Today.” Journal of Applied Security Research 11, no. 4 (2016): 517–25. <https://doi.org/10.1080/19361610.2016.1211876>. [↑](#footnote-ref-187)
188. USGS Human Capital Office, “Personnel Suitability Guidance Position Sensitivity and Public Trust Risk Level Determinations Q&A,” USGS, accessed November 6, 2022, <https://www.usgs.gov/human-capital/personnel-suitability-guidance-position-sensitivity-and-public-trust-risk-level-0#:~:text=Q%3A%20What%20are%20public%20trust,applicable%20laws%2C%20regulations%20and%20guidelines>. [↑](#footnote-ref-188)
189. “Intelligence Community Personnel Security Database Scattered Castles,” Intelligence Community Personnel Security Database Scattered Castles § (2020), pp. 1-3. [↑](#footnote-ref-189)
190. Josh Fruhlinger, “The OPM Hack Explained: Bad Security Practices Meet China's Captain America”. [↑](#footnote-ref-190)
191. “OPM Data Breach Part II,” OPM Data Breach Part II § (2017). [↑](#footnote-ref-191)
192. Ibid. [↑](#footnote-ref-192)
193. Aliya Sternstein and Jack Moore, “Timeline: What We Know about the OPM Breach (Updated)”. [↑](#footnote-ref-193)
194. Nicole Perlroth and Adam Goldman, “Chinese National Arrested in Connection with U.S. Cyberattacks,” The New York Times (The New York Times, August 25, 2017), <https://www.nytimes.com/2017/08/24/technology/chinese-national-arrested-cyberattacks.html>. [↑](#footnote-ref-194)
195. Adam Goldman and Eric Schmitt, “One by One, ISIS Social Media Experts Are Killed as Result of F.B.I. Program,” The New York Times, November 24, 2016, <https://www.nytimes.com/2016/11/24/world/middleeast/isis-recruiters-social-media.html>. [↑](#footnote-ref-195)
196. Erica D. Borghard and Jacquelyn Schneider, “Israel Responded to a Hamas Cyberattack with an Airstrike. That's Not Such a Big Deal.,” The Washington Post (WP Company, May 10, 2019), <https://www.washingtonpost.com/politics/2019/05/09/israel-responded-hamas-cyberattack-with-an-airstrike-thats-big-deal/>. [↑](#footnote-ref-196)