The Rise of Cyber Warfare

The Digital Age and American Decline

Hanyu Chwe

In May 2007, unknown attackers declared cyberwar on Estonia. Estonians woke up to find that the websites of their banks, newspapers, and government agencies had been systematically dismantled. This was one of the world's first cyberwarfare attacks; I argue that it won't be the last.

In the future, the amount of cyberwarfare will increase drastically. First, the increased value of cyberspace increases the incentives to wage cyberwarfare. Second, the logic of cyberwarfare nullifies several mechanisms that constrain territorial war. Finally, the offensive advantage inherent in cyberwarfare exacerbates the security dilemma. The United States lacks many of its traditional military and economic advantages in cyberspace; the increasing importance of cyberwarfare will accelerate the relative decline of American military power.

For the purposes of this paper, I define cyberwarfare as the use of computer programs to attack, disrupt, destroy, disable, or steal anything of military, economic or general strategic value or efforts to defend against such attacks. I am not considering industrial corporate espionage, cyber attacks meant to aid the use of conventional military force, or the use of internet media to organize social action. In my definition, cyberwarfare is not intentionally accompanied by corresponding actions in the real world.

Cyberwarfare Incentives

The strategic and economic value of cyberspace is huge. Facebook and Google were worth 200 billion dollars and 400 billion dollars in 2014 respectively. (Bloomberg.com, 2014) Billions of people use the Internet daily, hundreds of billions of dollars are traded yearly (Pew Research Centers, 2013)—cyberspace is lucrative. However, the value of cyberspace is limited in internet companies or transactions; almost every large organization uses the internet to communicate. (Meltzer, 2014) A corporation or government can be crippled by the loss of their digital infrastructure from suffering cyberattacks, Sony was completely shut down for four days. (Cunningham & Waxman, 2014) Four days of no internal communication in the American federal government would be a disaster. Few human activities don't go through the internet: it controls everything from our bank accounts to television shows, from Facebook to large swathes of the American power grid. (Tucker, 2014) A state needs to guard its cyberspace in order to ensure stability.

It's unlikely internet reliance will decrease. Humanity's relationship with the internet changes rapidly—as new technology develops, more opportunities exist for companies and inventions to affect our lives. For example, the rise of smartphones provided opportunities for dozens of new start-ups and another way for humans to interact digitally. (Dougherty, 2015) Finally, millions of people have yet to come online. In the United States, cellphone usage almost doubled from 2011 to 2014. (Pew Research Centers, 2013) Microsoft predicts that there will be 4 billion internet users by 2020, most new users coming from developing countries. (Cyber Trust Blog, 2013) As the internet population increases, the value of cyberspace will increase even more.

Cyberspace is valuable today and will almost certainly be more valuable tomor-

row.[1] States need to protect their own "digital territory" in order to shield their governments, militaries, and corporations from disruption. As the value of cyberspace increases, the incentives to wage cyberwarfare increase as well. The stakes have risen—states need allocate more resources to cyberwarfare, either in hopes of hurting other states or defending against attackers.

The increasing strategic value of cyberspace does not, by itself, imply a corresponding rise in cyberwarfare. However, the anonymous nature of cyberwarfare removes three causal mechanisms that discourage conventional conflict. Without these conflict-reducing effects, increased conflict becomes more likely.

No More Restrictions

Scholars have discussed multiple reasons for the current decline in conventional warfare. Unfortunately, three proposed explanations for why conflict is discouraged in the modern system are rendered invalid by cyberwarfare.

First, as hegemon armed with dominant conventional military force, the United States has the incentive and the means to quash weaker states' attempts to expand or balance against it. (Wohlforth, 1999) It is possible that the threat of American retaliation and intervention has prevented dozens of potential armed conflicts. Second, nuclear deterrence discourages war. The threat of mutually assured destruction prevented conventional warfare during the Cold War. Third, increased economic interdependence makes economic costs from war too high—the current system of global trade is so intertwined that few countries would gain from conflict. Any one of these factors, or more likely a combination, may drastically reduce conflict in the modern era. However, these obstacles simply don't apply to cyberwarfare.

For the first time in history, it is possible for a state to weather attacks that damage their military, economic, or industrial infrastructures and not be able to confidently determine the identity of their attacker. James Lewis states, "Identity is easily concealed in cyberspace...sophisticated attackers are skilled not only at hiding their identity but also making it look as if someone else was responsible". (International Relations And Security Network, 2009) Attackers can disguise their IP addresses or "transmit their attacks through multiple nodes of transmission" (Rattray, 2001, 66) in order to disguise themselves or blame other actors. It's almost impossible for cyber defenders to be completely certain about an attacker's identity—even if the evidence clearly points to one actor, it may just be an attempt to shift blame by a sophisticated attacker. Gregory Rattray adds, "Depending on the sophistication of the attacker, it's possible to leave the defender unsure if an attack actually occurred". (Rattray, 2001) The ability for attackers to completely disguise themselves completely topples conventional security logics.

Actors can attack in cyberspace without fearing retaliation. Without knowing the attacker's identity, the United States can't intervene. Similarly, if states don't know the identity of their attacker, nuclear deterrence is useless. It would be irresponsible to threaten nuclear reprisal over cyberattacks when it is so difficult to accurately determine the identity of the attacker. Even if the identity of the attacker seems obvious, it's impossible to completely rule out the possibility of another actor shifting blame onto an innocent party. Finally, in cyberwarfare, a state can

[1] I would argue that the value of physical space is decreasing as well. A full-fledged explanation is outside the scope (and word count) of this paper, but the decreased value of physical territory also increases the value of cyberspace.

attack another state and trade with it at the same time. States can engage in cyberwarfare without risking losses from trade; defending states wouldn't know with whom they should stop trading. Cyberwarfare doesn't invalidate all possible reasons for the reduction of conflict, but it completely dismantles three major ones.

By itself, the increased value of cyberspace and the increased ease of conflict doesn't guarantee more cyberwarfare. However, due to the offensive advantage of cyberwarfare, the security dilemma in cyberspace is greatly exacerbated. Even if states don't intend to wage offensive cyberwarfare, it is difficult for states to escape the security dilemma.

Offensive Advantage and the Security Dilemma

The security dilemma states that when states attempt to increase their security, they almost always inadvertently threaten other states. This causes other states to attempt to increase their own security, ultimately decreasing security for the first state and increasing the likelihood of conflict. There are two variables that tend to exacerbate or ameliorate the security dilemma.

First, the relative advantage of offensive weapons, tactics, and strategies over their defensive equivalents exacerbates the security dilemma. Robert Jervis explains that when offensive advantage exists, even status-quo states "must then act like aggressors; the fact that they would gladly agree to forego the opportunity for expansion in return for guarantees for their security has no implications for their behavior". (Jervis, 1978, 87) In a world with offensive advantage, it is difficult for states to defend themselves; the best way to maintain security is to attack. Clearly, this greatly exacerbates the security dilemma—if states are more likely to attack than defend, any perceived increase in military power is extremely dangerous. Furthermore, the expectation of easy victory increases the incentives for offensive war.

In cyberspace, offense has a clear advantage. According to Robert Ghanea-Hercock, "Offense is favored over defense... since only a single point of failure in a cyber network, or process, is required for a successful attack". (Ghanea-Hercock, 2012) Cyber defenders need to protect thousands of nodes in a network; attackers need only to gain access through one. Accordingly, the amount of code needed to construct defense towers over the few hundred lines of code needed to conduct an attack. (Singer & Friedman, 2014) Defensive programs cost more time, money, and effort. Not only is it easy to find holes in opponents' defenses, but the locations of those vulnerabilities is easily disseminated, making it easy for even unsophisticated attackers: Rattray says, "Widely used products contain vulnerabilities to digital disruption that are easily identified...the tools and techniques to exploit them are quickly disseminated among potential attackers". (Rattray, 2001, 470) Finally, offensive advantage is bolstered by the rapidly changing nature of cyber weapons. It's easy for attackers to design new weapons; when a government agency or corporation designs an effective counter to one offensive technique, several more weapons can be created. David T. Fahrenkrug says, "The current offensive advantage results from the ability to maneuver against a network combined with rapidly adaptive tools to attack networks and information". (Czosseck, 2012) Offense is more effective, easier, and cheaper.

Perception of offensive advantage is arguably more important than the actual existence of offensive advantage. After all, states act according to their perceptions of the world, not necessarily the real world. Major actors still believe that offensive has the advantage. In 2010, when describing the Pentagon's new cyberdefense strategy,

the U.S. Deputy Secretary of Defense made clear that "In cyberspace, the offense has the upper hand". (Lynn, 2010) Conventional wisdom favors the offensive in cyberspace.

The second variable that impacts the security dilemma is the perceivable differentiation between offense and defensive weapons or postures. If a state can see that other states are increasing their security through defensive means, it is less likely to feel threatened. The more differentiation, the more informations states have about other states' intentions.

Unfortunately, it is impossible to differentiate offensive cyberwarfare from defensive cyberwarfare. Investment in cyber warfare simply cannot be divided into offense and defense. Both involve investment in trained personnel and powerful computers. Personnel trained in cyber defense need to be intimately familiar with methods of attack in order to defend against them—it's impossible to differentiate between "offensive" and "defensive" cybersoldiers. Computers can be used for both offensive and defensive maneuvers. There is no meaningful distinction. The nature of the security dilemma makes cyberspace conflict more likely. In an offense-dominated world with no distinction between offense and defense, even status-quo states are likely to resort to aggression and cyberattacks.

In the 21st century, actors have the incentive and the means to increase cyberwarfare: the value of cyberspace will increase, providing incentives for offensive cyberwarfare, and several mechanisms that have traditionally constrained conflict won't apply, giving actors the opportunity to wage war. Even status quo actors will be unable to escape the security dilemma, causing more conflict. In a future characterized by increased cyberwarfare, the United States loses several key advantages.

American Loss

The United States loses its advantageous geographical position. The Atlantic and Pacific oceans form natural lines of defense for the United States and make conventional land attacks difficult. The United States' two neighbors have never posed substantial military threats, easing the path to regional hegemony. Furthermore, the United States' relative isolation enables it to possess substantial power without being incredibly threatening. Since a state's capacity to project power declines over distance, far off powerful states become less threatening than weaker neighboring states. If states do balance against threat and not necessarily power, as Stephen Walt surmises, then the United States is able to enjoy substantial military capacities without threatening other states and provoking balancing. (Walt, 1985)

Unfortunately for the United States, physical geography is irrelevant in cyberspace. The United States' "moats" won't dissuade cyberattacks. In cyberspace, all countries are neighbors —the United States' threat level will increase, sparking increased balancing against the United States.

Additionally, the United States' diplomatic advantage will be mitigated. More than any other state in the system, the United States benefits from a large network of formal and informal military alliances. However, since cyberwarfare confuses traditional definitions of war, the United States cannot rely heavily on alliances like NATO for support. For example, it's unclear whether a cyberattack on the United States would trigger NATO's collective security clause. Allies of the United States could shirk their responsibilities to the United States, arguing that cyberattacks do not constitute war. As cyberwarfare becomes more common, 20th century organizations have to adjust for a 21st century world. Traditional military al-

liances are less effective.

Furthermore, because of the nature of cyberwarfare, the United States' economic and military advantages are diminished. In this case, the disadvantaging effect of cyberwarfare does not apply only to the United States, but all conventionally powerful states. First, more technologically developed states are inherently more vulnerable in cyberwarfare. Large developed countries have more electronic infrastructure to defend; the larger your network, the more vulnerabilities you present to your attacker. Stronger actors have more to lose than weaker actors do in cyberwarfare.

The United States is "the society most reliant on its information systems and infrastructures". (Rattray, 2001, 8) According to Pentagon officials, "massive networking makes the U.S. the world's most vulnerable target for information warfare... The U.S. has orders of magnitude more to lose from information warfare than its competitors". (Clapper, 1997) Not only does the United States more vulnerable to attacks, but it also risks more when attacking—because American cyber infrastructure is so large, American cyber attacks can cause collateral damage to American digital infrastructure. (Rattray, 2001, 191) If the USA engages in sustained cyberwarfare, it simply has more to lose than any other actor in the system.

Second, the United States' great industrial and population advantage is diminished. Political historians often use industrial capacity and population to measure power—Paul Kennedy uses industrial and population measures to determine great power status in *The Rise and Fall of the Great Powers*. (Kennedy, 1987) The huge industrial capacity of the United States contributes to its status as hegemon. In cyberspace, however, industry and population are much less important.

In conventional warfare, the number of tanks or planes a state possesses is a good indicator of its military power. In cyberwarfare, the number of computers doesn't matter: "The tools and techniques used for digital attacks require relatively little capacity in terms of commercially available computational power, storage space, and transmission capacity". (Kennedy, 1987, 138) Cyber conflict privileges quality of programming, not necessarily industrial strength and material wealth. Individual programmers with outdated computers can wreak havoc. Rattray explains, "Some of the most disruptive viruses unleashed in the early 1990s were produced by students using computers with 286 processors at a technical high school in Bulgaria". (Kennedy, 1987, 138)

In the same way, the number of soldiers are less important in cyber conflict. Training and creativity trumps quantity of combatants. The infiltrators of Rome Laboratory, the R&D lab and technological heart of the United States Air Force, turned out to be a lone teenager armed with a home computer. (Kennedy, 1987, 138) Rattray mentions that "Human expertise and organizational coordination will likely prove the constraining factors in planning and execution of strategic information warfare attacks, not availability of hardware and software tools". (Kennedy, 1987, 138) The main quantitative constraint in cyberwarfare is the accumulation of enough trained individuals: "personnel shortages and changing skill requirements constitute a major barrier to successful information technology assimilation in the United States and elsewhere". (Kennedy, 1987, 178) To be sure, large industrial capacity and population don't hurt the United States—in fact, because of its large, well-educated population, the United States is more likely to produce talented hackers—but in cyberwarfare, they're much less important than they used to be.

In part because of the low quantitative requirements, the cost to enter cyberwarfare is low. Rattray writes, "The cost of acquiring the necessary means [for digital attacks] is low, especially in relation to conventional forces and most WMD alternatives. A much wider range of actors can consider employing such a form

of warfare". (Kennedy, 1987, 469) This diminishes the relative military advantage of the United States. Although highly-trained individuals are important, even a modicum of skill gives actors the ability to wage cyberwarfare: "acquiring the technical knowledge to conduct digital warfare has become increasingly easy". (Kennedy, 1987, 190) Cyberspace is the great leveling ground; actors without large populations or industrial might can wield undue influence. Because so many weak actors can participate in cyberwarfare, the United States' relative military strength declines.

Finally, it will be difficult for the United States to completely control certain regions of cyberspace. In territorial conflict, strong countries can attempt to secure strategically important areas in order to protect vulnerabilities or maintain prime attacking position. The United States can secure its borders or control the "commons"— the sea, air, or space. (Posen, 2003) However, it's impossible to completely protect "space" in cyberspace. Any connection in and out of a cyberspace "territory" is an another avenue for attack. In order to effectively protect such an area, the space needs to be completely isolated, rendering it effectively useless. Without the ability to completely secure spaces in cyberspace, powerful actors lose another advantage.

Some of the United States' advantages will translate beautifully into cyberwarfare. The United States is the most technologically advanced country in the world. It houses the vast majority of the world's top technical universities and internet companies. Those universities and companies are a major producer of top-level cyberwarfare talent.

The high skill level of the United States' cyberwarriors ensures that United States will be the strongest state in cyberspace, However, due to the United States' disadvantages, it is unlikely that the United States will enjoy dominance in cyberspace to the same degree that it does in real space. The United States is a conventional military hegemon; it will not be a military hegemon in cyberspace.

Conclusion

As seen above, states have two different military capacities; cyberspace military power and conventional military power. As cyberwarfare assumes a higher proportion of all conflicts, states' cyberspace militaries will begin to matter more than conventional militaries. This won't make America's conventional military edge completely irrelevant;[2] however, the United State's overall military dominance will diminish. Although the United States will still be the strongest state in the system, it will no longer enjoy military hegemonic status.

This paper predicts rampant cyberwarfare and a United States with diminished cyberwarfare capabilities. However, the continually changing nature of cyberspace makes prediction particularly difficult. Technological advances might remove anonymity and ensure effective retaliation. Internet predictions must consider the possibility of rapid change. Still, given present facts, increased conflict seems certain.

[2]In fact, it might be the case that the United States' overwhelming conventional military dominance discourages conventional war, thereby encouraging increased cyberwarfare.

References

Bloomberg.com. 2014. Facebook Valuation Tops $200 Billion. *Bloomberg*, September.

Clapper, James R. 1997. *Seminar on Intelligence, Command, and Control.* Cambridge, MA: Program on Information Resources Policy, Harvard U, Center for Information Policy Research.

Cunningham, Todd, & Waxman, Sharon. 2014. Sony Struggles to Fight #GOP Hackers Who Claim Stolen Data Includes Stars' IDs, Budget and Contract Figures. *TheWrap*, November.

Cyber Trust Blog. 2013. Linking Cybersecurity Policy and Performance: Microsoft Releases Special Edition Security Intelligence Report. *Cyber Trust Blog*, February.

Czosseck, Christian. 2012. Countering the Offensive Advantage in Cyberspace: An Integrated Defensive Strategy. *2012 4th International Conference on Cyber Conflict.*

Dougherty, Conor. 2015. Start-Ups Try to Challenge Google, at Least on Mobile Search. *New York Times*, May.

Ghanea-Hercock, Robert. 2012. Why Cyber Security Is Hard. *Georgetown Journal of International Affairs*, 81–89.

International Relations And Security Network. 2009. Discouraging Deterrence. *International Relations And Security Network*, November.

Jervis, Robert. 1978. Cooperation under the Security Dilemma. *World Politics*, **30**(2), 167–214.

Kennedy, Paul M. 1987. *The Rise and Fall of the Great Powers: Economic Change and Military Conflict from 1500 to 2000.* New York, NY: Random House.

Lynn, William J. 2010. Defending a New Domain. *Foreign Affairs*, September.

Meltzer, Joshua. 2014. Supporting the Internet as a Platform for International Trade. *Global Economy and Development at Brookings*, February.

Pew Research Centers. 2013. Device Ownership Over Time. *Pew Research Centers Internet American Life Project RSS*, November.

Posen, Barry R. 2003. Command of the Commons: The Military Foundation of U.S. Hegemony. *International Security*, **28**(1), 5–46.

Rattray, Gregory J. 2001. *Strategic Warfare in Cyberspace.* Cambridge, MA: MIT.

Singer, P.W., & Friedman, Allan. 2014. Cybersecurity and Cyberwar: What Everyone Needs to Know.

Tucker, Patrick. 2014. Forget the Sony Hack, This Could Be the Biggest Cyber Attack Yet. *Quartz*, December.

Walt, Stephen M. 1985. Alliance Formation and the Balance of World Power. *International Security*, **9**(4), 3–43.

Wohlforth, William C. 1999. The Stability of a Unipolar World. *International Security*, **24**(1), 5–41.