Erschienen in: Peace Economics, Peace Science and Public Policy ; 18 (2012), 3. - S. 1-11
https://dx.doi.org/10.1515/peps-2012-0006

DE GRUYTER DOI 10.1515/peps-2012-0006 — PEPS 2012; 18(3): 1-11

Proceedings of the 12th Jan Tinbergen European Peace Science Conference

Sebastian Schutte

Cooperation beats Deterrence in Cyberwar

Abstract: This brief article argues for a narrow definition of cyberwar and a technology-centric approach to understanding its strategic implications. Based on a review of the underlying technologies, approaches to facilitating peace in this rather new form of confrontation will be derived. This brief discussion already shows that Cold War era strategies such as credible deterrence through retaliation are ill-suited to serve peace in the digital domain. Generally, building offensive capabilities for cyberwar does not increase an actor's security. Instead, geographically unrestricted security communities (Deutsch et al., 1957) of nation-states that employ similar technologies seem to serve individual security best.

Sebastian Schutte, E-mail: schuttes@ethz.ch

1 Introduction

How would we know a civil war if we saw one? This simple question asked by Sambanis (2004, 816) underlines that concepts of political violence are not necessarily self-explanatory. While the problem of identifying civil wars is considerable, it is much harder to identify so-called "cyberwars". There is a lot of confusion about the shape, meaning, possibilities, and limitations of these forms of "warfare" due to the infancy of the organized military exploitation of digital technologies. Equally problematic for the study of cyberwar is the fact that empirical material is sparse and anecdotal, such that standard methodology cannot be applied. As a result and despite considerable public and military interest, peace and conflict research on cyberwar has not gained much traction. This article applies a narrow definition of cyberwar that offers more conceptual clarity than previous definitions: *cyberwar is understood as the exploitation of weaknesses in digital communication technology with militarily relevant kinetic consequences.* The advantage of this definition is that it is more specific than the related concepts of information war, cyberactivism, and computer-based espionage. Moreover, the definition directly builds on the technological pre- requisites for cyberwar. As will be argued below, three technologies need to converge (and have most recently converged) in

order to speak of cyberwar. By reviewing the technological foundations of cyberwar, strategic implications of this new form of conflict can be derived. Analogies to the physical domain will be used to contrast differences between the domains. Most importantly, this purely theoretical discussion can already serve to show that well-established strategic constellations such as credible deterrence under perfect information or security dilemmas are less likely to arise in this form of war. The article therefore serves as a first step in terms of providing a conceptual point of departure for future empirical research.

2 Cases of cyberwar

A series of high-profile hacks with kinetic consequences and military goals have recently made headlines around the globe. One interesting chapter was added to the continuing tensions between Iran and Israel in 2010 with regard to Iran's allegedly civilian and possibly military nuclear program. A piece of malware, later called "Stuxnet", was discovered and finally underwent a lengthy analysis by Microsoft Research (BBC, 2010). The surprising conclusion was that the software had been crafted to exploit no less than four previously unknown security vulnerabilities in Windows systems to artfully alter the code running on industrial control systems that steer uranium-enriching centrifuges (Naraine, 2010). Instead of bringing these systems to a halt, the injected commands were designed to both ruin the current uranium batch and damage infrastructure by continuously slowing down and speeding up the centrifuges. The spatial distribution of infected systems indicates that the attack had been launched in a targeted manner against Iran and is widely assumed to have succeeded in slowing down the Iranian nuclear program (Sanger, 2012). This particular incident is most closely related to an earlier militarized interstate dispute in the region: In 1981, Israel successfully bombed an experimental nuclear reactor in Iraq that it suspected of generating weapons-grade uranium (Perlmutter et al., 2008, xxix). The bombing of the Osirak nuclear reactor in Iraq and the complex digital attack on the Natanz nuclear facilities in Iran clearly indicate that kinetic attacks and digital manipulation can sometimes be used interchangeably to achieve political goals "by other means".

But Iran did not have to wait for too long before it could point to its own first successful cyberwar operation. In December 2011, an American RQ-170 UAV (Unmanned Aerial Vehicle) that operated in Iranian airspace was brought under Iranian control and then skillfully crash-landed near the city of Kashmar. Damage to the aircraft was minimal and it was displayed on national television days later.

Evidence of what actually happened is very sparse, but one plausible scenario involves Iranian personnel having jammed the radio frequencies used for communication between ground control and the vehicle (Hecht, 2011). In such situations, UAVs might resort to navigating back to base autonomously, relying on GPS radio navigation. GPS receivers calculate their own position and altitude by measuring the exact time of receiving time-stamped radio signals sent from orbiting satellites. Since these signals are unencrypted and the frequencies are known, ground-based senders could in principle overpower the satellites' signals and send GPS messages in carefully selected intervals. This sort of GPS "spoofing" is very difficult to apply in a controlled manner, but technically feasible. Theoretically, navigation could have been controlled from the ground by essentially telling the aircraft that it was already back to base. Historically, this incident closely resembles other militarized interstate disputes, such as the 1962 downing of an American reconnaissance plane over Cuba and similar incidents in Soviet airspace (Polmar, 2001, 181 ff.). Again, by slightly different means a digitally executed attack (instead of a surface-to-air missile in this case) served the same end as an act of war.

These two cases described above belong to a new category of digital attacks with immediate kinetic consequences. With little imagination, cases of this type can be assumed to take place more frequently in the future as unmanned and remotely operated vehicles become more common on the battlefields. While two cases are an insufficient basis for empirical research, a review of the underlying technological prerequisites of cyberwar in general can lead to substantial theoretical insights and replace a largely speculative debate on future forms of cyberwar with a deductive approach.

3 Existing research

Given the lack of systematic research and sparse empirical evidence, current research usually applies established concepts from the realm of interstate war to the digital domain. This trend probably started with Arquilla and Ronfeld (1993), who extensively used analogies and examples from military history to generate a suitable intuition for what cyberwar might look like. Vacca (2011) observed that the struggle over responsibility and resources for the establishment of a US "cyber command" is marked by the historical roles and doctrines of different arms branches. While inter-service competition is a long-standing phenomenon, the debate over who should defend the US at this new and crucial front seems to be marked by different classic approaches to warfare, according to Vacca. Mahan's

(1892) emphasis on keeping the sea lanes open in the case of war and Douhet's (1921) focus on the offensive power of the airplane indeed suggest very diffeent starting points that can also be applied to cyberwar. In a comprehensive study on cyberwar, Libicki (2009) asks specifically whether strategic concepts from interstate war could be implemented successfully in the digital domain. Contrasting the Cold War environment of a global nuclear stalemate with two superpowers interacting under near-perfect information, Libicki (2009, xvi) concludes that credible deterrence based on reliable second-strike capacities did not have an obvious equivalent in the much less clear domain of cyberwar. Clarke and Knake (2010, 6) opt for a more inclusive definition of cyberwar, also covering attacks that remain in the digital domain. But their discussion of approaches to managing the risks associated with cyberwar are well founded and largely free of attempts to apply Cold War strategies to the digital domain.

4 Technological prerequisites for cyberwar

While most current approaches try to derive strategic approaches to cyberwar from kinetic analogies, this article analyzes cyberwar based on the underlying technologies. As will be shown in this section, three technologies are necessary for bringing about cyberwar as defined above.

4.1 Von Neumann Machines: Processing (and confusing) data and instructions

In the early post-WWII years, the crude calculation machinery used by the Western Allies to break German and Japanese encryption codes had reached a certain level of maturity. Building on earlier theoretical work by Turing (1936) that had formally defined the prerequisites for freely programmable computing machinery, the American ENIAC (Electronic Numerical Integrator And Computer) was widely perceived as a seminal platform (see: Van der Spiegel et al., 2000) still provided two different memories: one for instructions and the other for data. The distinction of these two memories made data and instruction handling considerably easier from the hardware layout point of view. It nevertheless made the programming of complex applications much harder from the programmer's perspective. John von Neumann, a brilliant Hungarian-American mathematician mostly known for his contributions to Game Theory, closely followed the progress of the various computer research groups in the US. Already in 1945 he proposed

a new general architecture that featured a common memory for instructions and data. This architecture is known today as the "von Neumann" architecture and essentially every modern computer implements it. The "von Neumann" architecture provides full flexibility to the programmer. The data processing capabilities of the computer can be used to generate instructions. Computer programs can be executed from the internal memory, as well as altered or copied using a different program. While this unification of data and instruction memory is a great practical leap, it can be exploited to covertly execute instructions hidden in data. While this seems to be a rather abstract problem at first glance, memory safety violations account for a substantial percentage of all IT security vulnerabilities. This problem is of course greatly increased in the Internet age since data transfers occur on a permanent basis globally. Limiting data connections, for example by breaking individual links between nodes, is not a strategy that can resolve this essential problem, as the next section will show.

4.2 TCP/IP: Fault-tolerant communication

The looming threat of an all out nuclear war and the identification of second-strike capabilities as a prerequisite for stability led to research on fault-tolerant communication technology in the 1960s and 70s. Defense research funding was therefore spent on researching network technologies that would enable arbitrary end-to-end communication in digital networks, even as links and nodes were constantly removed by nuclear bombardment. The corresponding technology formally first proposed in 1974 still powers the Web of today: TCP/IP (Cerf and Kahn, 1974). Some of the fundamental characteristics of TCP/IP include detecting transmission errors and resending data packages, automatically adapting to maximal transmission speeds, and the possibility of circumventing broken network links through dynamic routing. This enables TCP/IP-based networks to ensure end-to-end communication between nodes in digital networks as long as one route exists between them. This fault-tolerant architecture is still an essential part of the modern Internet. With the rapid growth in bandwidth and decline in round trip times, the Internet and various application layers built on top of the underlying network technology have created a system that essentially looks like a fully connected network in terms of allowing almost any node to talk to almost any other node through a series of routers and networks that are invisible to the user. While this progress provides the basis for the digital media revolution, it has also outlived its initial strategic environment. Instead of powering communication among trusted nodes under the pressure of kinetic thinning of the network, untrusted nodes spreading malicious code throughout a network that cannot

be turned off or controlled in its entirety is the underlying problem of cyberwar. Targeted attacks against remote hosts have essentially replaced the "computer viruses" that spread slowly via floppy disks in the 1990s. And while everyone from nation-states to uprisings enjoys the advantages of resilient communication today, everyone is also at risk of being attacked by other network nodes.

4.3 Do-by-wire: Remotely and digitally controlled systems

Remotely operated vehicles and industrial machinery are by no means new inventions (Singer, 2009, 47-48) But the combination of embedded von Neumann computers, GPS navigation, and advanced wireless digital communication have given rise to a whole series of modern unmanned vehicles being deployed in large numbers on today's battlefields. While military operations might appreciate the system's integration of digitally connected vehicles, ground stations, and troops in the field, one must remember that freely programmable von Neumann machines and resilient network technologies underlie these systems. The discussed cases of manipulating unencrypted GPS signals and reprogramming industrial computers highlight the fundamental insecurity of this setup. Replacing older analog steering technology through digitally-connected control-by-wire systems comes with great economic advantages. But it also entails the general possibility of systems being compromised through the exploitation of digital vulnerabilities. The crucial implication for cyberwar is that a successful attack in the digital domain can bear immediate kinetic consequences.

5 Strategic Implications

This section discusses the strategic implications of cyberwar based on the review of underlying technologies.

5.1 From physical destruction to covert control

In a rarely remembered, but perfectly practical definition of warfare, Boulding (1962, 266) reasoned that war could be roughly defined as men throwing things at each other with malicious intent. Following this insight, Boulding traced the development of destructive capabilities in history in terms of projectiles being thrown at ever increasing distances: "It starts with rocks, and it advances to spears

and arrows, to cannons and rifles [...] and airplanes with bombs and guided missiles and nuclear warheads." This refreshingly simple and yet perfectly accurate summary of millennia of armed combat illustrates how cyberwar deviates from traditional warfare with regard to two central aspects: space and sophistication. For the realm of physical destruction, Boulding (1962, 245) proposed a formalism that expresses a decline in strength as a function of distance. According to Boulding, this decline in strength becomes smaller and smaller as history progresses and the range of carriers and projectiles increases. In the digital realm, the loss of strength as a unit of distance has finally vanished completely. Digital code can be transported effortlessly and instantly around the globe. But the ability to transport code across digital networks does not in itself represent a successful cyber attack. Instead, a carefully selected chain of vulnerabilities in foreign systems must be selected and exploited. While digital communication with target systems can usually be established easily, taking control of these systems is a completely different challenge that requires sophistication, background knowledge, and previous experiments in test environments. Establishing contact with attack targets in the traditional kinetic domain is a greater problem where spatial separation provides the primary obstacle and destruction is the primary goal. Once this contact is established, however, destruction is a lesser problem. Destroying physical infrastructure through the detonation of explosives or the collision with fast-moving projectiles is a very simple principle. Getting a foreign system to execute code that it assumes to be data is a more difficult challenge. The purpose of the projectile is blunt destruction, while the purpose of the cyber attack is sophisticated manipulation with more remote kinetic consequences. The building blocks of information theory (Shannon, 1948) can be used to loosely illustrate this difference: kinetic destruction usually aims at adding entropy to physical systems in terms of blowing them to pieces. The system's possible states after detonation are increased by orders of magnitude in comparison to the possible states prior to detonation. But cyber attacks do not increase entropy in the same way. Instead, they increase the difference between a digital system's true state and the one expected by its operators. This increase in false expectations could be better expressed in terms of relative entropy.

5.2 False Flag attacks and paranoid attributions

The changed immediate objective of acquiring remote control rather than causing physical destruction follows another strategic implication: uncertainty of origin. In most kinetic scenarios, the attack leaves a smoking gun of some sort. Radar recordings and used munitions reveal the country of origin in conventional air

strikes; different forms of remote sensing and military reconnaissance allow the identification of foreign troops and navies. This means that many militarized interstate disputes start with aggressive rhetoric, followed by troop mobilizations, and finally violence. With regard to cyberwar, the element of surprise is of crucial importance and the analysis of the origin of an attack is essentially reduced to much less efficient forms of computer forensics. Identifying the attacker, the attack vector, and the damaged caused by the attacker while in command of the compromised system can only occur after an attack has been detected. In many scenarios this will only be the case after an attacker has accomplished his goal and possibly covered his tracks. For all practical purposes, political actors might not be able to identify the origins of acts of cyberwar beyond a reasonable doubt. In these situations, actors might resort to the "cui bono" heuristic and attribute the attack to those strategic adversaries that benefit most. Especially in multipolar settings, this is arguably the most dangerous aspect of cyberwar — it opens a possibility for false accusations with little technical leverage to prove innocence. Similarly, false flag attacks can be easily implemented by placing hints at a false origin of attack on compromised systems. Strategies of retaliation can therefore be used to induce confrontations between actors by third parties, and do not seem well suited to serve peace in the digital domain.

5.3 Offensive capacity correlates with defensive vulnerability

Another counterintuitive aspect of cyberwar is that offensive capabilities usually correlate with defensive vulnerabilities, a point made by Clarke and Knake (2010, 155) specifically with regard to the US. As any successful attack requires the identification of previously undisclosed vulnerabilities, societies with a large IT infrastructures produce tech-savvy individuals that use methods to find new vulnerabilities and write and sell exploits. Of course, such societies tend to be wealthy and most easily set aside the resources needed to build offensive cyberwar capabilities. At the same time, such states are much more vulnerable to cyber attacks than less developed states which employ non-computerized industries and weapons systems. This effect again runs against the intuition from the physical domain: for example, societies with highly developed industrial complexes and civilian car industries are more likely to develop armored vehicles and usually possess them in large quantities. But while industrial strength translates into security from foreign occupation, high reliance on computerized systems translates both into the strength to carry out attacks as well as a high vulnerability to foreign attack. A low-tech army can be overrun, but not hacked. A high-tech army can be hacked, even if it is capable of hacking and overrunning others. The silver

stripe here is that the classic logic of a security dilemma which is largely believed to have propelled some of the most lethal arms races in history does not hold for cyberwar.

While sophisticated attacks such as those carried out by Stuxnet require active research on exploitable vulnerabilities, turning these exploits into attacks does not automatically enhance one's own security. Instead, security can be best increased by patching existing vulnerabilities. In pursuing this goal, security communities of states that employ similar technologies could emerge. Such long-term international cooperations could easily pay for newly discovered attack possibilities and then share the acquired knowledge among them. Moreover, existing solutions to IT security such as virtualization, sandboxing, good firewall designs, and reliance on open source software could be applied that guarantee security without relying on offensive capabilities. Deterrence is again a misleading analogy and security cannot serve as an excuse for building offensive capabilities.

6 Discussion and Conclusion

As argued above, a narrow definition of cyberwar relies on at least three separate technologies that have converged recently in digitally controlled industry and weapons systems as the result of long-standing historical trends. With regard to the strategic aspects of cyberwar, this brief theoretical contribution has attempted to show three things. First, there is indeed a set of cases of militarized interstate dispute in which digital attacks have clearly replaced kinetic attacks, and these can be called cyberwar. Second, due to the infancy of cyberwar, the current discussion on cyberwar is still hopelessly stuck in the Cold War and rather fruitlessly attempts to apply analogies from interstate war to the new concept. Third, a suitable starting point for deducing strategic aspects and policy approaches to cyberwar involves a careful review of the technological foundations of cyberwar and their implications. This focus on technology can also pave the way for empirical investigations. A simple event-dataset could be constructed around incidents of digital exploits that led to kinetic consequences. Some of the ideas discussed here, such as the positive correlation of capacity and vulnerability, could then be tested empirically.

A most important policy conclusion is that offensive capabilities do not enhance security directly because the ability to attack others does not automatically improve defense. Similarly important is the fact that credible deterrence is undermined due to the inability to attribute attacks to international actors.

Relying on deterrence in the digital domain is likely to come at the unacceptable risk of third parties inducing conflict through false flag attacks. Instead, states are in the historically unprecedented position of building security communities which are independent of geographic constraints. Through international funding, states could buy and disclose exploitable vulnerabilities and thereby enhance their own security without having to rely on offensive capabilities. A technological aspect of cyberwar working against this optimistic outlook is the complete inability of any political actor to monitor the development of offensive cyberwar capabilities on a global level. Cyber attacks that might require less spending than new kinetic weapons systems can be developed in complete secrecy. But international actors would still be well advised to simply out-bid attackers by contributing to a large security community that finds and patches vulnerabilities before attackers can exploit them.

References

John Arquilla and David Ronfeld. Cyberwar is Coming! National Defense Research Insitute, 1993.

BBC. Stuxnet worm hits iran nuclear plant staff computers. BBC News; Available online at http://www.bbc.co.uk/news/world-middle-east-11414483, 2010.

Kenneth Boulding. Conflict and Defense: A General Theory. Harper, 1962.

Vinton C. Cerf and Robert E. Kahn. A protocol for packet network intercommunication. IEEE Transactions on Communications, 22(5):637_648, 1974.

Richard A. Clarke and Robert Knake. Cyber War: The Next Threat to National Security and What to Do About It. HarperCollins, 2010.

Karl Wolfgang Deutsch, Sidney A. Burrell, and Robert A. Kann. Political Community and the North Atlantic Area: International Organization in the Light of Historical Experience. Greenwood Press, 1957.

Giulio Douhet. Command of The Air. Air Force History and Museums Program, 1921.

Jeff Hecht. Did iran capture us drone by hacking its gps signal? New Scientist; Available online at http://www.newscientist.com/blogs/onepercent/2011/12/did-iran-hack-us-drones-gps.html, 2011.

Martin C. Libicki. Cyberdeterrence and Cyberwar. National Defense Research Insitute, 2009.

Alfred Thayer Mahan. The Influence of Sea Power Upon History. Dover Publications, 1987.

Ryan Naraine. Stuxnet attackers used 4 windows zero-day exploits. ZDnet Blog; Available online at http://www.zdnet.com/blog/security/stuxnet-attackers-used-4-windows-zero-day-exploits/7347, 2010.

Amos Perlmutter, Michael I. Handel, and Uri Bar-Joseph. Two Minutes overBaghdad. Routledge, 2008.

Norman Polmar. Spyplane: The U-2 History. MBI Publishing, 2001.

Nicholas Sambanis. What is civil war? Journal of Conflict Resolution, 48(6): 814_858, 2004.

David E. Sanger. Obama order sped up wave of cyberat- tacks against iran. New York Times; Available online at http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all, 2012.

Claude E. Shannon. A mathematical theory of communication. Bell System Technical Journal, (27):379_423, 1948.

Peter Warren Singer. Wired for War. The Penguin Press, 2009.

Allen M. Turing. On computable numbers, with an application to the entscheidungs problem. Proceedings of the London Mathematical Society, 42(2):230_65, 1936.

Alexander W. Vacca. Military culture and cyber security. Survival: Global Politics and Strategy, 53(6):159_176, 2011.

J. Van der Spiegel, J. F. Tau, T.F. Ala'ilima, and L. P. Ang. The eniac: History, operation and reconstruction in vlsi. In R. Rojas, editor, The First Computers: History and Architectures. MIT Press, 2000.