PARTNERSHIP FOR PEACE CONSORTIUM
POLICY BRIEF

Evolving Approaches to Cyber Defense

PfPC Emerging Security Challenges Working Group Policy Brief No. 7, December 12, 2016 | www.pfp-consortium.org

EXECUTIVE SUMMARY

This policy brief examines cyber defense and the policy issues associated with their evolution.

The unprecedented increase of interconnectivity during the last decades has brought new challenges to cyber defense. The ubiquity of information and communication technology in everyday life rightly creates concerns to experts responsible for national security. Despite the relatively strong protection of military and governmental assets, civilian infrastructure is often vulnerable to cyber attacks. However, a disruption in one leads to disruption in others. Cyberspace thus has become a domain which can be easily exploited by hybrid warfare tactics implemented by state and non-state actors alike.

Therefore, states have to adapt their policies to be able to cope with these new challenges. The issues for policy consideration include efforts to strengthen national cyber defense capabilities, building trust among the relevant stakeholders, fostering cooperation with the private sector, clarify legal frameworks, and to establish measures to keep pace with new cyber challenges.

Introduction

Phone Phreaking, computer hacking and cyber attacks have been around as long as the technology they exploit. The Computer Chaos Club was formed in Germany in 1981, the same year the first IBM Personal Computer was released. The media reports on the cyber defense threats of 2016 are echoes of media reports of worms and botnets in 2006 and viruses in 1996. Those responsible for cyber defense are locked in a Red Queen's race. Governments, acknowledging increasing diversity and consequent unpredictability of cyber threats, are building up their cyber defense capabilities. However, to be successful, current approaches to cyber defense need to be reviewed and constantly adjusted to new realities in the cyber domain.

New cyber challenges impacting national security

As societal reliance on information and communication technologies grows so do concerns among experts responsible for national security. Despite the relatively strong protection of military and governmental assets, civilian infrastructure is often vulnerable to cyber attacks. With critical infrastructures and services increasingly online and interconnected, there is a greater risk for cascading effects – if one is disrupted the higher the likelihood is that others follow suit. As a result, vulnerabilities in the private sector could easily transform into national security vulnerabilities. The cyber domain therefore offers good opportunities for state and non-state actors to create strategic erosion, e.g. by using non-kinetic means to erode an adversary's

willpower and the cyber space has become a vital component of hybrid warfare.

The Internet of Things (IoT) illustrates this point well. While IoT promises to make our daily lives easier, it also enables the collection and communication of extensive amounts of data, creating new opportunities for malicious actors. IoT devices are often not sufficiently protected and can be used as entry points to networks for hackers with intentions to compromise information and/or disrupt the functioning of their target. The October 2016 Distributed Denial of Service (DDoS) attack on Dyn[1] via the Mirai botnet practically illustrates how IoT devices can be utilized for malicious purposes. Over fifty companies, media outlets, and governmental departments were affected.

Over the last years, attacks on stock markets, banks, and other financial institutions are also becoming common place, as is corporate espionage. Western countries, relying on cyberspace for their day-to-day operations, are particularly vulnerable to this type of attack. For example in 2014, a cyber attack caused physical destruction at a German steel mill by disrupting the industrial control system (ICS) for the blast furnace, preventing its proper shutdown and causing extensive damage. Internet connected ICS are prevalent throughout industry and represent a tempting target for adversaries.

The vulnerability of civilian infrastructure has not only been exploited by criminal individuals or organizations but also by states. Currently, some nations may be investing in the development of small cyber teams of hackers who can compromise civilian targets. The development of small cyber militias may become a future "weapon of choice", especially in countries with limited conventional capabilities.

With a similar objective, the spread of psychological operations in cyberspace is likely to continue and intensify in the next decades. Such operations create desired narratives with a goal to manipulate the audience and leading to doubts and spread of fears among the targeted population.

There are other developments which may be even more worrisome. For example, South Korea has openly admitted that it has built cyber weapons that can be used to attack North Korea's nuclear weapons facilities. Attempts of North Korea to infiltrate nuclear power plants in South Korea are no less frightening. Earlier this year, attacks on a Ukrainian nuclear power plant caused new wave of concerns. These types of activities are particularly dangerous as cyber attacks do not always work the way they are planned. Consequences associated with cyber attacks on nuclear facilities can be wide ranging.

However - barring attacks on nuclear arsenals - it is unlikely that cyber attacks will be singularly decisive in a future conflict. They are likely to take place along more traditional kinetic elements, aiming to provide an advantage in time and space by targeting the weakest links of the security chain. Thus, given more interconnected devices and more well-funded adversaries – the cyber defender has to be increasingly proactive to maintain a certain level of defense. At the NATO Summit in Warsaw in 2016, the Allies recognized cyberspace as a domain of operations, acknowledging that NATO must defend itself in cyberspace as it does in the air, on land, and at sea.

Policy recommendations

1. *Strengthen national cyber defense capabilities:* State-of-the-art cyber defense a decade ago is only the starting point of cyber defense today. Already in peace time, nations must continually improve their ability to prevent cyber attacks; defend against large-scale cyber attacks; educate, train and exercise cyber defense; and assess the effectiveness of their cyber defense programs in order to limit cascading damage.

2. *Build trust:* As malicious actors are forming coalitions and discovering innovative ways of sharing information and expertise, cooperation with external stakeholders becomes a

[1]Dyn is a cloud-based Internet Performance Management company.

critical necessity for national cyber defense. However, to achieve such cooperation and collaboration, trust is an indispensable ingredient. A starting point is the establishment of networks in which each stakeholder has a point of contact.

3. *Foster cooperation with the private sector:* The establishment of trust does not pertain to the public domain alone. Equally important is to establish public – private trust. It is understandable that states only reluctantly pass their responsibility to provide security for its citizens to the private sector. Nevertheless, public-private partnerships are cornerstones of cyber security – especially as the majority of critical infrastructures and services are managed by the private sector. To mitigate these tensions, national strategies should highlight the importance of public – private partnerships. Governments can provide support and coordination through the establishment of regulatory frameworks for ensuring accountability, responsibility, and resilience while allowing industry to stay flexible and react to new developments in the cyber domain.

4. *Clarify legal frameworks:* Despite the recognition that international law applies in cyber space (UN GGE), there are still divergences among countries as to how it applies in specific situations. For example, the Tallinn Manual acknowledges the lack of concrete guidance on cyber warfare. Instead of proposing new cyber legislation, it interprets international humanitarian law and its applicability to cyber operations in war time. Similarly, the US Department of Defense's manual on law of war contains specific references to cyber operations. But rather than setting up new concepts of international cyber law, it notes that states should focus on a number of issues that remain unanswered in interpreting the broader international law, such as the problems connected with the difficulties in negotiating terminology or verification of compliance with adopted treaties. While efforts to clarify legal frameworks is needed, it should be recognized that it may lead to further tension down the road as countries find certain positions to be in strong opposition to their own.

5. *Establish measures and policies to keep pace with new cyber challenges:* The rapid evolution of cyber threats means that policies to implement national strategies, have to adjust to new circumstances. Over the last years, policies focused mainly on finding the right balance between security and privacy needs for individual users. Today, addressing this issue is not sufficient; even as it itself has become more nuanced through the recognition the need to take into account a human rights dimension. The international community faces a broader spectrum of cyber challenges that can impact the availability (e.g. the DDoS attacks on Estonia in 2007 and Dyn in 2016), integrity (for example as a result of the cyber attack on Ukraine's electricity grid in 2015), and confidentiality of services and data – most recently observed during the 2016 U.S. Presidential race.

This brief is mainly based on presentations, discussions, and subsequent interactions of the Emerging Security Challenges (ESC) Working Group held in Kiev, Ukraine, on 14-16 September 2016. The contributing author is Ms. Jana Kotorova, Science for Peace and Security (SPS) Programme Officer, NATO.

The ESC Working Group is chaired by Dr. Gustav Lindstrom, Head of the Emerging Security Challenges Programme, Geneva Centre for Security Policy and Mr. Michael Gaul, Senior SPS Programme Advisor (Projects & Strategy), NATO.

CONTACT INFORMATION

For more information on the activities of the PfP Consortium's Emerging Security Challenges Working Group (ESC WG), please contact the PfP Consortium Secretariat by email at:

info@pfp-consortium.org or visit our website at: www.pfp-consortium.org