TRANSATLANTIC CYBERSECURITY

119

THE ONLY WINNING MOVE IS TO PLAY WITH OTHERS

Charly Salonius-Pasternak & Jarno Limnéll

FIIA BRIEFING PAPER 119 ▪ December 2012

U2FsdGVkX19597Gtuu65sO0pV4Cp+y2QLCyDHWfK1WKmKUfWDzV/hq0Z/h8282prAEFWIcUmNbVYGUPvuClRNIalPKuaAQYvgJSGqypyBFwQIiRJdS2a5evHn/yRYMyReVJLQC
84NAwTMo6Ij9B4QyLaDDUs7LuU7Y4tSVlqKG5vO2XGf2SGq2L0hZWOHTG8fxvdVZtXpl1zRUpA3w7iiC9XTKlpzhzYZq8sITY3G30KKCZxXMawTr595dkhFgwluJdyb/EJFBm1jqdHj231u/
Fn+xi5MnkSidb8vwMAixPan3Do0y0qLcr7dpir2d0YkFRgbAqY3bVPJZZu [illegible] q6gfZhjZneALucvZuLuTwhV37WODxcHjqWf+FVwSxB4/IUEea7bUwOfDXRTiglMdSoLb+/e/K0x-
UZk633xOE++EKPztiyHkLqY7Aquy1xAmBA5y77totI7O+18lWfAW2GFq1V [illegible] 36fpzwMtLa6ICmVejpfFFAxjcabzVgHW5DJKWsyblAdOanutrLnd3k3hnH1xG/neSLH+YU+IUg/
MaovsADL7dUiuZiIRUO1OBmrX3Yeeyhel15euEBofUrWeGROdl3zDAEz8icw [illegible] 'F/pvG03wXjH15wPYOdT4wXg3oqCVQI0eZugLY3c5/K86P9TMfemH30A
2J1QB14a2uX44A88lfD8rFuxbtiJQ5BpM6OdcrXib7tTuJ1fmujjoGX7s1bIkdgGQ5qN90yk7gU [illegible] 'qG4D6qWP [illegible] fyt+rne7xhZUzSlOXsp7NCIUk4gyihjRV+lFfw3EKdBH
fTE377yjAnv5jFckpPM3rR5V78fnxMBvhhLCZ9Y2SJU4PT09dsTGCx49AAOv2FTeK6VveUJNeSI9 [illegible] Kml [illegible] 3GfrSG+GBgjV7kbEPoBbZvR9rDu9+226U72o5y
dBMvg7CszQtb0KWW2yvGk2u0TLoE4p+s1v38YhMXDQRt8hewkVwnZCB05HKI/KGhb2JJwlDr5I [illegible] /gN5cyGfbzESJM4JK4aNmyBgke9VGmPlH+0CsI
wV0JX1v5ZSr41hAZOqaDBqVstZ5ug7PLxxQXcuOJQMhV6WtCLeKe8gkoNE+rXXHMGMScA8z3nh [illegible] Wcw/HZTBgLHiIHlLaPAVBNmGGaDKYQYxK2INZx
IcWSiX29uUjDNYXHyWsCevbz3uIE15ZP8cAzGS05I480xwJFb2o73Sx3Q7Eaz0QgI31vbp6C [illegible] _Ob' [illegible] wquS+e7RUnPHzSux2LtWae+rKtkBz8u
01ny0xkR8aXPrOgndRemZRSE+FV1D+R1ZtxOnMMTDqT9CO/oEpFmhotiOsPSqLlPH [illegible] Q7U' [illegible] ,t2X368BBv2vci6e1IeNRbFnkg4KnicU78
VpB5B7fmFhRV88VHr4VDFK4txaV/4n7cF3swqlN7uVBEOK2BS5qJzNl+LSGoaT [illegible] vPugjMT4^ [illegible] ĺpU7EqwbCbfMqsjjG0p4kqTDsLsL4VJZ2eg7I
1SAwGJ7BNMQKWE5VLWSq6rF5l4CDFchJq0hwiqmVrvlOlzeGbDsDkxTY6P [illegible] .ĺSwS5pVAsrzrN1aZjR5tLoT1im+/vMSuycymWHqm6
R2C9xVyP3o0oldGROm4nq5G4uwMjlCoj2+AUNLqq9ARSBIAlhJOVG [illegible] JJrIWr1 [illegible] ,nI7TKWd0vno04lr404XSziYdtsi3FHZwq61C/5fAlqPxS5s
3e8bJd2l6YAhuepSoIIJFJOZN+Q3uD2r2joTXSeb3mLKMspEjrQ67K [illegible] ɟlGx+9/tU3NzUzUS, [illegible] ¿ᵖp4d/QyXTGg9ODe415zsRWciPzv3NYAHaZfnx6vExxs4lt2Ghy5
HrJw6AYEp0l+apzDAd6vuTyRb+B3QlXPsIIXTXmHPZJ4pWflOZ1fh [illegible] 'Ct7tTTHtF5+/BxKlUONDrxND9G02yeDsRA5AEyMMBv+Ozk4kH8d5uYBavthS1Mho3
wvuhsKVnHExllX6pTKVW4z6mhWbjtwsAqUE6mtpIjsN95v2 [illegible] i8Q4Y4QMEqyzB/yZ6xvrwQ6LaFF2aj4WwPaQCviM9pKa6DMkDUQ7Gd0+1pAOJkd
EqGmpX8O5R/lcz4m/d5qB6leQeoRfov+TEvEH1GocARUh [illegible] 9LMOXjLxsv6wcLixz5mNlYLd4SZXaTZPQfPAdM4h3WVjZu1ro4Ub2q5K3CsC7jnyol
0kBycJxZvrB49xMo59lbTV/gqkhawQDydn4uNqnRo [illegible] ĸd3r1IDfEIGvGNEXWDVwMMDSHpdd5qhRu9LaGtHwYHE6a0ETUNjeISwKzFBV5LW
6pqpCrETyuriGWOL8Lt2mSNS7pv5ZnD7S782T [illegible] ŕ05TwqjϑL [illegible] hzJswNOEEJL0V62c/nzJqSXpcvpL+ocdw/+D+aGfeon1/vO2h6CVojAeJywLjA3oC
sTpftURp3cFbWlJIVB7PtVN9SqYstvHlkjsdOGF [illegible] ĸXVQL [illegible] lh3ehetyTvltj6lxwo [illegible] ,vz8DjE3jnTR1N3f8A+FWxzd33A73qh3+NFQh0qepbrrrYWtTYfRQEPdaNxN9+kMdkE
RjqojdqJ0XXQkSEXkCzscmhm8svXwzF+ [illegible] ,ŁWXQGDGwh0kWMc2K5ppqS6Dnbu5nADQ1Wr7LM14kBtMLAdZ4XFtMdcjo4Rl19es08vWtWfltyP0xRrGXKrQ6nXfOesQ==SBIAlhJO
VGaiYtdrhS+x2Exz1cUSkSAFMP2r [illegible] .ɯsEkhHVIfB0rnl7TKWd0vno04lr404XSziYdtsi3FHZwq61C/5fAlqPxS5s3e8bJd2l6YAhuepSoIIJFJOZN+Q3uD2r2joTXSeb3mLKMspEjrQ67KVN
rO5B38d9YdGLG6cP4kvszqlGx+9/ [illegible] SynQPp4d/QyXTGg9ODe415zsRWciPzv3NYAHaZfnx6vExxs4lt2Ghy5HrJw6AYEp0l+apzDAd6vuTyRb+B3QlXPsIIXTXmHPZJ4pWflOZ1fbPVaBF59KM/
jX2o0md6BV48ZX8qCt7tTTHtF5+ [illegible] ONDrxND9G02yeDsRA5AEyMMBv+Ozk4kH8d5uYBavthS1Mho3wvuhsKVnHExllX6pTKVW4z6mhWbjtwsAqUE6mtpIjsN95v2KuifJKfyuSXtY0tLTT
6KpVfHmteUYgOwi8Q4Y4QMEqyzB, [illegible] vrwQ6LaFF2aj4WwPaQCviM9pKa6DMkDUQ7Gd0+1pAOJkdEqGmpX8O5R/lcz4m/d5qB6leQeoRfov+TEvEH1GocARUhubtfcucLa5kuvd9cFVEeu
0U4QWus58J9o9LMOXjLxsv6wcLixz5mNlYLd4SZXaTZPQfPAdM4h3WVjZu1ro4Ub2q5K3CsC7jnyol0kBycJxZvrB49xMo59lbTV/gqkhawQDydn4uNqnRogvD3jd/515HsjpVIp5GXHv8j6Q

ULKOPOLIITTINEN INSTITUUTTI
UTRIKESPOLITISKA INSTITUTET
THE FINNISH INSTITUTE OF INTERNATIONAL AFFAIRS

TRANSATLANTIC CYBERSECURITY

THE ONLY WINNING MOVE IS TO PLAY WITH OTHERS

Charly Salonius-Pasternak
Researcher
The Finnish Institute of International Affairs

Jarno Limnéll
Doctor of Military Science
Director of Cyber Security, Stonesoft Corporation

FIIA Briefing Paper 119
December 2012

- Cybersecurity concerns everyone, and is everyone's responsibility. It is a genuine example of a society-wide security issue.
- The United States is ahead of Europe in discussing and integrating (military) cybersecurity into its foreign and security policies. For the US, the biggest challenges at the moment are: updating legal frameworks, creating cyber rules of engagement for the military, building cyber deterrence and clarifying the cybersecurity roles and responsibilities of government and private sector actors.
- Cooperation at national and international levels is integral to improving cybersecurity. This includes updating international and domestic legal frameworks to ensure that state actions are accountable, and to protect citizens from wanton strikes at critical infrastructure.
- Governments must hold private sector partners accountable, and through partnerships ensure that societal cybersecurity is not overshadowed by private interests – public-private partnerships have a crucial role to play in this.

Global Security research programme
The Finnish Institute of International Affairs

ULKOPOLIITTINEN INSTITUUTTI
UTRIKESPOLITISKA INSTITUTET
THE FINNISH INSTITUTE OF INTERNATIONAL AFFAIRS

Cyberspace has become an important arena of world politics. Cybersecurity has political, security and economic dimensions which further blur the concept of conflict; perpetual (cyber) conflict could become the norm. The digital world has become a domain where strategic advantage can be won or lost, the latter being more likely without serious indigenous cyber capabilities. In short, every modern country in the world is creating cyber capabilities, with the result that the global military security landscape has not changed as dramatically since the advent of nuclear weapons.

Cyber capabilities will soon be essential for nation-states and armed forces that want to be treated like credible players. Due to its exposure and interests, the United States is currently at the forefront of conceptual, ethical and political discussions about cybersecurity. Having spent at least a decade integrating the cyber world into its security and military thinking, it has also taken the lead in using cyber attacks as a tool of foreign and security policy, thereby placing it far ahead of Europe, where discussion about offensive cyber capabilities, for example, is hushed in many countries. Most European countries have cyber strategies on paper, but public discussion and practical measures at policy and doctrinal levels are not as mature as they are in the United States.

The difference between the United States and Europe is notable, and without serious efforts in Europe, the gap is only likely to widen. This would increase the potential for Europe to become the focal point for serious cybercrime, espionage and even debilitating attacks. Europe would be foolish not to follow and learn from such a key actor in the cyber world. As in many security issues in general, there are signs that in cybersecurity the default for most Europeans seems to be to follow US approaches and guidelines.

Recognizing the futility of a 'government only' approach, the US has sought to harness the skills and motivations of the private sector so that when they are combined with state efforts the overall cybersecurity of the US is improved. Government officials and private sector advisors in the US are currently grappling with four key challenges:

1. Updating legal frameworks
2. Creating cyber rules of engagement (ROEs) for the military and societies
3. Attempting to build effective cyber deterrence (especially against non-state actors)
4. Seeking to clarify the roles and responsibilities of federal and private sector actors in cybersecurity and preparedness.

Overview of US cyber efforts

The United States has striven for years to better integrate various elements of cybersecurity and weapons into its political-military toolbox. It has demonstrated operational cyber capabilities, but is struggling to create a coherent whole out of its diverse cybersecurity efforts. As a focal point for its military efforts, the US Cyber Command was created in 2009, achieving initial operational capability in May 2010. The Cyber Command has responsibility for military networks, while the Department of Homeland Defense is responsible for other government networks, but would in practice lean heavily on the military in the event of a large-scale attack. The private sector provides both these government actors with extensive services, including the development of offensive cyber capabilities.

The number of cybersecurity attacks and probes against the US government and firms responsible for critical services has increased dramatically. The head of the US Cyber Command and head of the National Security Agency (NSA), General Keith Alexander, has said that between 2009 and 2011 there was a 17-fold increase in such attacks. He also rated US defensive preparations for a large cyber attack at a three, on a one to ten scale.

These trends have occasioned US officials to frequently talk about the growing potential for a "Cyber 9/11" or "Cyber Pearl Harbor". The purpose of these references is to both highlight the damage that a cyber attack could cause in the physical world and to prepare the population for such an attack. The shrill tone of the warnings also reflects a particular American sense of vulnerability which is not always based on reality. More positively speaking, these officials frequently focus on recovering from such attacks – namely on resilience – rather than speaking about being able to prevent them completely. This is clearly a part of an ongoing redefinition of threats regarding cybersecurity.

Cyber weapons and their attractiveness

The cyber domain should not be treated as a separate domain but one that is intertwined with the physical space. As an increasing number of people and objects are digitally connected, the cyber domain expands and becomes more complex at every turn; the integration of the cyber world with the physical world will give humanity a new dimension of life. Our dependence on the digitalized world has increased to such an extent that for all developed and most developing economies, normal life has become impossible without it. This great dependence on bytes has also developed into a genuine weakness – one which many actors around the world want to exploit. Critically, from a military perspective, the difference between kinetic and non-kinetic environments will become more blurred and in many respects will merge into one.

The actors involved also continue to evolve. The threat of a lone hacker popularized by Hollywood movies has given way to various virtual 'cooperatives' and professionally organized entities. Unlike in the case of conventional military capabilities, these non-state actors can and do challenge far larger states, highlighting the potential systemic impacts of the emergence of the cyber domain. States recognize this, but have only recently begun to actively develop and resource the development of cyber capabilities.

At present, more than 140 countries have indicated that they have programmes to militarize cyber capabilities. The most extensive such efforts can be found in the US, China, Russia and Israel. Though benefits of scale and computational power available to states still apply, the reality of cybersecurity is that even the smallest actors can contribute to the largest. The best hackers in the world can cause more damage than thousands of good coders. Those same individuals can also create a suite of cyber tools to be deployed by thousands of less skilled national cyber soldiers. In international cyber conflicts small states and non-state actors can potentially have far more significant roles than in the physical world.

Cyber weapons are attractive for a number of reasons, and for three in particular. First, due to the very nature of the cyber world (especially the technical structure underpinning the Internet), the offence-defence balance is heavily tilted in favour of offence. Second, it is possible to cause equivalent damage through investments that are orders of magnitude cheaper than using conventional weapons. Third, while physical weapons can almost always be identified, cyber weapons provide a new level of deniability.

The fear of an existential attack and growing international activity in the cyber domain has focused US official minds on four key challenges.

Four key cybersecurity challenges the US is tackling

1) Updating legal frameworks

Mirroring its concern that private sector firms are the most vulnerable and potentially most lucrative targets of cyber operations, the Obama Administration recently sought to pass an amended Cyber Security Act of 2012 which would, among other things, have set minimum standards for cybersecurity and created a form of reporting to ensure compliance. Because the bill was not passed, President Barack Obama signed Presidential Policy Directive 20, allowing the military to prepare for and act using both defensive and offensive measures if either the federal government or important private sector actors were targeted in a serious cyber attack.

According to reporting by the *Washington Post*[1], the directive differentiates between general network defence and cyber operations, as well as spelling out responsibilities between federal agencies. The directive further clarifies which cyber domain operations can be undertaken by whom in the government, thereby taking tentative steps to address the second key challenge facing US officials – creating rules of engagement.

1 Ellen Nakashima, "Obama signs secret cybersecurity directive, allowing more aggressive military role", *Washington Post*, November 14, 2012.

2) Creating cyber rules of engagement for the military

Cyberspace is considered by governments to be the fifth domain of warfare, in addition to space, land, sea and air. As such, militaries and their political masters demand clear and understandable rules of engagement (ROE). What makes the creation of these ROE difficult, among other things, is that although cyber combat has some stand-alone qualities, it exists in the political and strategic context of warfare, of the physical world.

More critically, the 'equivalencies' of different actions are not clear; especially when actions cross the physical-digital divide. Can the same ROE allow for a cyber attack that degrades digital network performance, while disallowing an attack using physical weapons on a key communications node? Currently, even if the initial impact were the same, it is likely that the cyber attack would not be viewed as an act of war by another state actor.

Considering these and other challenges, it is not surprising that the US has struggled to create clear rules of engagement. Moreover, even if the United States managed to create ROE, without global cooperation they may even cause further instability. The reason is that there is also a dearth of globally accepted concepts that would undergird the creation of cyber ROE. The need for such concepts is apparent if one considers the physical world, where Chinese and US Navy ships may not know their respective ROE at any given moment, but the general concepts of what they may be are understood by both sides.

3) Building cyber deterrence

In every domain of warfare, it is imperative to build some level of deterrence, which consists of a combination of doctrine of use, real capabilities, and others' awareness of those capabilities. Building cyber deterrence (which by definition are capabilities that others are not able to see) is a tough challenge for the US. Just talking about defensive and offensive cyber capabilities in general terms, without revealing or demonstrating those capabilities does not advance deterrence. This can effectively be contrasted with nuclear deterrence, where capabilities are well understood by all sides; yet even here the usefulness of the concept of deterrence against non-state actors must be challenged.

In the US, cyber deterrence is currently seen to consist of a triad. The first leg of this cyber triad is resilience. In practice this means that the US must build resilience into different systems and procedures, so that adversaries know that they cannot succeed in crippling the economy, government, or US military with cyber attacks. The task is to convince others that no actions they take will paralyze the United States.

The second leg of the new Cyber Triad is attribution. It is difficult to identify the ultimate source of cyber attacks – this is the problem of attribution. If enemies can attack a country´s networks without identifying themselves, they can attack with near impunity, making deterring them practically impossible. The United States is expending considerable resources to be able to confirm the ultimate sources of attacks and probes more rapidly; doing so in ways that can be publicized only adds to the challenge.

The third leg of the Cyber Triad is offensive capabilities. Just as with kinetic weapons, opponents must know that a potential target state possesses effective offensive capabilities and is ready to use these capabilities – if needed. The idea of offensive capabilities is no longer an issue in the United States, with the discussion now focusing on how and what capabilities should be (further) developed. The logic behind offensive weapons, which is applicable to Europe, is that offensive capabilities are necessary to build a robust defence and to support the building of deterrence and confidence in the armed forces' capabilities in the cyber domain.

The ultimate goal of cyber deterrence-building is that states, terrorists and rogue regimes realize that the US digital infrastructure is resilient, that the US can accurately identify any attackers, and that it can fully defend itself in cyberspace or through other means.

4) Clarifying the cybersecurity roles and responsibilities of public and private sector actors

There is an increasing awareness that governments and private sector firms must cooperate for cybersecurity to be effective. US government officials understand that cooperation must take place in at least three spheres: real-time information sharing of threat pictures, the coordination of initial responses, and recovery – with resilience again

being a key attribute of cybersecurity. The ways in which this cooperation occurs, and under what legal or contractual constraints cooperation is placed, is only beginning to be grappled with. For example, when US Cyber Command observes an attack on a US-based financial institution, it is unclear how it should respond, whom it should inform, what assistance it could provide and what the private sector firm would want in terms of government assistance.

Following Presidential Policy Directive 20, the primary role of the US government is relatively clear when discussing extensive cyber attacks (comparable to an act of war) initiated by other sovereign states, even though the main target is likely to be critical private sector owned and operated infrastructure. However, the roles and responsibilities are considerably less clear during normal/peacetime periods when the problem is more one of cyber espionage, theft and disruption. General Alexander summarized the current environment by saying that cybercrime and cyber espionage constitute "the greatest transfer of wealth in history".

To begin combating this, Public-Private Partnerships (PPPs) are viewed as essential to a rational and functional cybersecurity approach, even in the United States. Some American politicians are concerned with imposing additional regulations on companies, but most companies themselves admit that they lack the resources and knowledge to fight aggressive attempts to steal intellectual property, especially when opponents (thieves) are supported by other states. By acting as clearinghouses for shared information and providing guidance on security, as well as counter-espionage capabilities, states can greatly assist the private sector. The focus of initial PPP efforts is likely to be firms that are involved in operating critical infrastructure, military contractors or those firms which create significant intellectual property.

What to absorb from US experiences and approaches in cybersecurity

During the next three years, cybersecurity-related discussions in Europe will take up issues that are currently being discussed and addressed in the United States. The discussions must engage society at all levels because cybersecurity affects society at all levels. These discussions must result in actions across Europe on the following six items:

Cybersecurity is a comprehensive societal security issue, and is a perfect example of the need for comprehensive societal security approaches. Cybersecurity concerns everyone and everyone is an actor, from the sustainers of the global financial system to individual smartphone users. This, coupled with the need for good public-private cooperation, implies that cybersecurity must be popularized. Everyone can grasp the concept and everyone must consider and discuss it to heighten awareness of its many facets.

Global and regional cooperation is an imperative; the only winning move is to play – with others. Cooperation is necessary globally, between smaller likeminded groups of countries and within states. By its very nature, cybersecurity requires strong cooperative structures and relationships. A key question is with whom we should increase and deepen cooperation. What are the practical and motivational connections that will bring likeminded countries together to cooperate? Moreover, which actors should take the lead both regionally and globally? Cooperation has inherent dangers, but it ultimately increases resilience, which is vital for a robust society-wide approach to cybersecurity.

Complete safety and security is an illusion, resilience is essential. We are highly dependent on digital networks, and consequently more susceptible to disturbances they cause in the real world. The importance of resilience cannot be overstated. Resilience must be built into technologies and processes. However, special attention must be paid to improving 'human psychological resilience' in situations where our lives are severely disrupted due to network failures. It is also vital to keep security in mind (from day one) when different technical solutions and protocols are being developed for the cyber world. To date, security has largely been an afterthought in this domain.

Public-Private Partnerships are compulsory in cybersecurity. Governments and the private sector are jointly responsible for building sound cybersecurity within states. Protecting critical national infrastructure is an extremely important aspect of cybersecurity. Securing this critical infrastructure, which in most western countries is owned

by private companies, should therefore be the first priority of national cybersecurity programmes. To facilitate this, mechanisms must be created through which society can benefit through the state from the best 'cyber wizards', who predominantly work for the private sector. These mechanisms should ensure assistance is available both in peacetime, as well as during emergencies and wartime.

In Finland, a history of cooperation and legal provisions created for a large reservist military can form the basis of an initial solution. However, small countries such as Finland must also contend with the reality that they have relatively little to offer large multinational companies when discussing public-private partnerships. On a national level, however, even large multinational companies can be mandated to take specified precautions in support of national cyber strategies, which include following minimum security standards and building resilience into daily business operations.

Building deterrence is necessary, including offensive cyber capabilities. Every state or alliance of states needs some level of deterrence to be credible. The discussion must also address the question of who will build these capabilities – every state, an alliance of states or the private sector? Should it be legal for private sector firms to sell one-use offensive cyber weapons to the highest bidder? In the sphere of military cyber defence cooperation, the only logical partner for European states, including Finland, is NATO.

Domestic and international legal frameworks must be modernized. These provide both national and international limits and create certain expectations of behaviour. States should aim to create international cyber rules of engagement concepts and guidelines, and potentially seek some limitations on the use of cyber arsenals against each other. Prospects for pre-emptive strikes must also be addressed. Such cooperation is necessary to avoid uncontrolled escalations and spirals of reprisals that shift impacts from the digital to the physical domains. This necessitates discussing how automated cyber counter-attacks can be. Discussions on legal frameworks also require extensive societal debate on the evolving balance between privacy and surveillance. States must cooperate globally to clarify and potentially seek some limitations on the use of cyber arsenals against each other.

The Finnish Institute of International Affairs
tel. +358 9 432 7000
fax. +358 9 432 7799
www.fiia.fi

ISBN 978-951-769-366-0
ISSN 1795-8059
Cover: Juha Mäkinen
Language editing: Lynn Nikkanen