Deutsch
Security Square

Security Brief
01
2015

FACULTY
OF SOCIAL SCIENCES
Charles University

Cyber threats should be assessed with a cool head

Nikola Schmidt

Ph.D. candidate at the Institute of Political Studies, Faculty of Social Sciences, Charles University in Prague

Background

In recent years, drawing attention to highly publicised episodes such as the cyber attacks in Estonia in 2007 or the sabotage of Iranian nuclear installation by the virus *Stuxnet*, may have been painting a future in shape of so-called cyber war; a new phenomenon in the world of international security characterised by futuristic combat where *bits* are taking over the role of *bullets*.

This brief seeks to straighten the perspective that is used in assessing new cyber security environment. The issue is of course a real one, but it is inappropriately approached. The point made here is not to overestimate the threat which leads to over-reaction in terms of strengthening current or developing new institutions to tackle cyber threats, and rather to engage in striving to better understand of what the cyber threat in fact is; how does it develop; change in time; how the cyber capabilities are detectable and thus predictable; and why we are wasting time by drawing doomsday scenarios that might never fulfill.

Analysis

The roadmap of current policy-making in cyber security is determined by emphasising selected extreme cases. Making them into ‘normal’ occurrences is by principle mistaken. Estonia was not prepared on DDoS (*distributed denial of service*) attacks in 2007, which caused paralysis of this digitalized society, because nobody expected an adversary willing to conduct such an attack. However, Estonia is much better prepared today and repeating the attack would likely not cause any significant harm. Tallinn has focused on better network topology, decentralized the information network and widen hierarchy of the connected systems and developed basic cyber defenses which significantly increased resilience of its critical infrastructure.

Stuxnet as an example of the attack capable of disturbing or destroying centrifuges in nuclear installations is also often interpreted as a ‘game changer’. However, first, intelligence agencies of powerful states have been in the front line of application new technologies for sabotage purposes for ages (take surveillance satellites as the first objects put in the Earth’s orbit as an example); second, the attack featured an insider who helped to bridge the gap between nuclear sensitive installations and office computers connected to the internet, and so it was not purely dependent on cyberspace operations. In fact, it was a state-of-the-art covert action combining traditional intelligence methods and brilliant piece of code that was tailor-made particularly for this attack. So, on a closer inspection, it is not a game changer, at least we have not witnessed more comparable attacks to date. Their conduct would likely remain limited only to the most capable intelligence agencies in the near future.

There are visible evidences how the threatening language of decision makers have influenced the development of this new agenda of national security and how it has shaped policy solutions to newly emerging threats. This is almost common wisdom in the field of sociology of technology governance that for example pays an attention on how epistemic communities are transferred into an epistemic authority the expertise and thus recommendations of are taken for granted.

We do not suggest that cyber security is not a domain that raises new and important questions for national security or defense. The fact that hacking satellites is an ordinary problem strikes this point home. However, the current intensive research should be more focused on openly accessible technologies and the development of knowledge to use them not only by states, but also by individuals for terrorism purposes. Strengthening the role of state institutions does not produce such knowledge, does not detect the development of specific knowledge empowering individuals to conduct attacks against critical infrastructure and does not give us proper knowledge how to assess the current cyber security threats that might significantly influence stability of our liberal democratic system as a whole. Moreover, the epic troubles that might be caused by cyber attacks to critical infrastructures can be solved by decentralization and system resilience. This approach significantly lowers the probability of cyber "Pearl Harbor" scenarios as then there will not be any "central mind of the humanity" to be paralyzed. Ideas such as these pave the way for merging traditional strategy with the novelty brought about by new technologies in interdisciplinary research instead of the mere straightforward application of traditional thinking on new cyber threats.

In addition, we are witnessing at the present time how the social media can be seriously used as a weapon in new kind of propaganda; as a tool of Russian one's foreign policy, which might have significant impact onto the way how local citizens assess their democratically elected government, thus directly impacting on the credibility of liberal democratic system. The recent Russian experience has shown that the cyber weapon does not need to destroy nuclear centrifuges or cause an electrical blackout to seriously destabilize democratically established countries, all without firing a single bullet, and avoiding a direct violation of international law.

We have also seen how a group of two, three or five people are capable to steal millions of credit cards and paralyze the top businesses for a period of time, producing huge economic loss. We also have seen some picturesque usage of the most common devices such as USB as an undetectable devices just by switching how they look like to the computer in their firmware (from a USB memory stick to a keyboard that causes avoidance of antivirus analysis and thus detection), but they might have significant applicability in corporate or government espionage and thus be used by barely experienced hackers that found the way to conduct such crime just a week before it is committed. Without better understanding of this infinite row of technology application to realise one's will in cyber space instead of leaning on several extreme but also *unique* events and drawing exaggerated, but also unrealistic, scenarios, we will never be able to think through reasonable policy solutions to these risks.

Bottom Line

- The way of developing useful knowledge for decision-makers in the cyber security domain is to support interdisciplinary research where policy-making meets the everyday expertise of technically oriented professionals in communications systems;

- Such combination will be beneficial by means of creating realistic scenarios and detection of actual game changers that may produce next extreme-*cum*-unique events;

- Policy makers should avoid simplistic views based on several "chosen" events including drawing doom scenarios based on the assumption that "everything is possible";

- Knowledge of information systems and the possibilities of their exploitation should be developed by interdisciplinary teams comprising social and ‘hard’ scientists, but also practitioners.

- Such cooperation would produce reasonable policy perspective that would be most likely to prevent unexpected events or maximise resilience of targeted systems.

Security Briefs are policy analyses published by the Deutsch Security Square, Institute of Political Studies,
Faculty of Social Sciences, Charles University in Prague. Visit us at deutschsquare.net.