EXTENSIVE TRANSPARENCY AS A PRINCIPLE OF CYBERSPACE GOVERNANCE AND CYBER SECURITY DILEMMA PREVENTION

Iulian F. POPA
Ph.D. candidate, Intl. Relations and Security Studies Doctoral School
Babeș-Bolyai University, Cluj-Napoca
ifp2@georgetown.edu

ABSTRACT
BEYOND DOUBT THE HUMANITY HAS ENTERED AN AGE OF DATA DOMINANCE. AS THE NEED FOR SAFETY AND PREDICTABILITY GROWS, IT BECOMES INCREASINGLY DIFFICULT TO BALANCE SECURITY AND INDIVIDUAL FREEDOMS. THE BALANCE BETWEEN SECURITY AND CIVIL LIBERTIES IS NOT CONSTANT AND PERFECT, GIVEN THAT THE EXPANSION OF SECURITY CHALLENGES TENDS TO BE INVERSELY PROPORTIONAL WITH THE BROADENING OF INDIVIDUAL FREEDOMS IN CYBERSPACE. INFORMATION AND KNOWLEDGE IS MUCH GREATER TODAY THAN IT EVER WAS. UNDER THESE CONDITIONS, MAINTAINING A PROPER BALANCE BETWEEN CYBER SECURITY AND USERS LIBERTIES MIGHT BE CHALLENGING AND DIFFICULT TO ACHIEVE. HENCE IN THIS PAPER I UNDERSCORE THE NEED FOR EXTENDED TRANSPARENCY AND COOPERATION IN CYBER EARLY WARNING IN ORDER TO INCREASE THE QUALITY OF CYBERSPACE GOVERNANCE THROUGH PUBLIC PRIVATE POLICIES FOCUSED ON OPEN AND TRANSPARENT INTELLIGENCE COLLECTION.

KEYWORDS*: CYBER SECURITY, TRANSPARENCY, CYBERSPACE GOVERNANCE, CYBER LIBERTIES.*

Introduction

Although years ago it would have been expected data expansion to lead to a safer and equitable world, this goal is still distant, even though recent studies showed that humanity can produce over 2.5 billion gigabytes each day – several times more than the total amount of data generated two decades ago in a whole year [1].

At the moment, I strongly believe the lack of equilibrium between security and freedom in cyberspace is not caused directly by the users' rights and freedoms, but by the way security is done to "protect" them. Largely the
response to cyber threats, risks, and vulnerabilities is most often influenced by an objective "state of affairs" and is motivated by the way it is subjectively interpreted. Therefore the general principles at the base of cyber security do not seem to differ substantially compared to other security dimensions – since all depend on intelligence collection and analysis. Therefore, by analogy with the land, air and sea, one may appreciate that the way cyber early warning is effectively done is of vital meaning for maintaining a proper balance cyber security and cyber liberties.

1. Transpancy and the cyber scurity dilemma

Concerning early warning, transparency plays a key role in ensuring a durable cyberspace security. As it influences to a significant degree the uncertainty among competitive actors it seems that lack of transparency or is one of the most significant elements which may facilitate the initialization and escalation of a cybersecurity dilemma. Hence the lack of transparency regarding intelligence collection and (mass) surveillance may pose serious unfortunate consequences to the durable development of cyberspace beyond doubt.

As I have underscore previously when tackling the cyber security dilemma [2], the data and information circulating in cyberspace are often a pretext for competitive actors to engage in security spirals or in low-intensity cyberwars due to their natural desire to acquire more power, prosperity, and security. Given the fact that partaking the security dilemma depends on subjective internal and external stimuli which competitive actors take into consideration, we can consider that there is a bi-directional cause-and-effect relationship between the initiation and the escalation of a cyber security dilemma and the way early warning is done on the other side. Therefore I believe that transparency in early warning (data and information collection and analysis) is of vital importance for the initiation and escalation of the cyber security dilemma, because once the dilemma has been initiated, its escalation becomes highly unlikely. Of course such situation disadvantages the non-combatants also or peaceful users of cyberspace whose cyber security ecosystem is seriously affected by the tensions and clashes between the cyber security dilemmas actors. Nonetheless, I noticed that the lack of transparency in early warning is highly likely to suppress many of the cyber liberties that non-combatants enjoy at the moment.

Long story short, compared to other strategic domains, I have noticed that the need for transparency in intelligence collection and exchange should not differ substantially in cyberspace. Of course, slightly different are the means and tools used in cyber early warning. From this point of view, I agree on the need for agility, flexibility, and unified standards is case of cyber security and cyber defense, as the absence of them may increase the odds of a cyber dilemma escalation and may decrease predictability as the tensions between actors grow due to "too much competitiveness". In fact, in cyberspace too much competitiveness may have an adverse effect on a long-term basis, due to the significant broadening of the disparities between actors and their cyber capabilities.

2. The need for extended transpancy

Obviously, 100% transparency is practically impossible and may not even be recommendable as total transparency in terms of security seems highly unfeasible.

On the other hand, from the perspective of good governance, an extended transparency model in early warning may be feasible, in order to offer sufficient guarantees for a peaceful and durable cyberspace development. Although it may pose several disadvantages on a short-term basis, an extensive transparency may generate positive effects for cyber security on a medium-and long-term scale. For instance, extensive transparency may contribute to a drop in both the tensions between the participants in a cyber security dilemma and in the threat level to the cyber liberties of non-combatants. Here the cyber security dilemma shows us that the lack of transparency stimulates competitive actors to develop and use clandestine tools for intelligence collection – as part

of their cyber proliferation programs, thus harming the users' cyber liberties and the neutrality of cyber technologies. We should not forget that in early 2015 the Kaspersky company documented and published important information on the spectacular capabilities of a certain malware was able to remain undetectable – once inserted into the firmware of home devices – and illegally transmit data from the infected devices to others being under the control of a supposed governmental agency[3]. In fact, as many other sources have revealed several classified information on the sophisticated tools used by a series of competitive actors to clandestinely compromise cyber terminals I would not insist on that.

3. Transparency as the first step towards a peaceful resolution to the cyber security dilemma

The first step towards a peaceful resolution of the cyber security dilemma is that transparency to be the rule and only in exceptional circumstances a breach of the rule.

Extensive transparency presupposes the use of data mainly in a peaceful way and in the benefit of durable development cyberspace. Therefore, collecting, exploiting and using data by means that breach rule are contrary to the good governance and cyberspace and should be highly avoided. In fact, transparency and the use of open data do not compromise the idea of security, given that they can contribute to the gathering of more significant and accurate intelligence.

Also, we should bear in mind that the idea of extensive transparency is gaining acceptance among many of the global decision-makers [4] as it fosters the durable development and neutrality of ICT and cyberspace. Actually, I suggest that neutrality and non-proliferation of cyber weapons are essential as they reduce the disparities between competitive actors as well as they concur with the peaceful resolution of the cyber security dilemma.

The advantages posed by open source data for security purposes are remarkable. It is broadly accepted among analysts that open source data have now a greater relevance than in the past. For example, the researchers from the University of Tennessee have been able to predict the location of Osama bin Laden prior to his capture by processing over 100 million open source data through techniques of geo-fencing and semantic analysis. Here some recent experiments confirm that data regarding the state of mind of online users might be used to predict in the future the appearance of great social movements, such as the Arab Spring [5]. Actually, the use of such advanced techniques of data analysis is not very uncommon, since they are frequently used by suppliers of online services or by the social networks in order to gather data and anticipate trends on how to deliver data tailored to the interests of the users.

Concluding remarks

Indeed, both the cyber security dilemma and good cyberspace governance confirm that the he role of traditional cyber security and defense means (e.g. in depth or perimeter-based) tend to decrease, as underscored previously [6], as long as they fail very often to optimize the agility highly demanded by nowadays security and cyber defense architectures.

In this sense, I observed that the integrated solutions (e.g. Big Data-based) for cyber security and cyber defense are increasingly attractive, since they can overcome many

of the operational flexibility faults posed by the traditional cyber security classic architectures still operating nowadays.

Long story short, some of the experts were right [7]. Ideally, in addition to in-depth cyber defense, a cyber security and cyber defense system would be able to real-time analyze any data and bits of information concerning the risks or anomalies of cyber defense, while simultaneously extracting tendencies and generating warnings before risks can produce operational losses. In that sense, collecting and using data in a clandestine manner, without a well-specified target, can increase the number of false-positive alarms and can harm the consistency of the tendencies, as well as the detection and neutralization of anomalies. It is not data collecting which is the most difficult aspect of rational security building, but rather the correlation and analysis of the data in order to ensure an optimal level of prevention. By optimal prevention I understand less false-positive alarms, increased resiliency, and reasonable guarantees for continuity ensuring.

REFERENCES

[1]. IBM, *What is big data?*, available at http://www-01.ibm.com/software/au/data/bigdata/, accessed on March 12th, 2014.

[2]. Iulian F. POPA, "Mapping the Cyber Security Dilemma. Selective Theoretical Remarks", in *The XXth International Conference Intelligence in the Knowledge Society*, Bucharest, Mihai Viteazul National Intelligence Academy, October 17, 2014, proceedings available at http://ssrn.com/abstract=2516268, accessed on March 12, 2015.

[3]. Kaspersky Lab, *Equation Group: The Crown Creator of Cyber-Espionage*, available at http://www.kaspersky.com/about/news/virus/2015/equation-group-the-crown-creator-of-cyber-espionage, accessed on March 3, 2015.

[4]. United States President, *Big Data: Seizing opportunities, Preserving values*, 2014, available at http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf, accessed on March 12, 2015.

[5]. Nathan Kallus, „Predicting Crowd Behavior with Big Public Data", în *International World Wide Web Conference Committee (IW3C2)*, Seoul, April 7–11, 2014, pp. 625-630, available at http://www2014.kr/wp-content/uploads/2014/05/companion_p625.pdf, accessed on December 12th, 2014.

[6]. Sam Curry et al., „Big Data Fuels Intelligence-Driven Security", în RSA Security Brief, January, 2013, pp. 2-3, available at http://www.emc.com/collateral/industry-overview/big-data-fuels-intelligence-driven-security-io.pdf, accessed on March 12th, 2015.

[7]. Alex Woodie, „Big Data at the Heart of a New Cyber Security Model", disponibil http://www.datanami.com/2013/07/03/big_data_at_the_heart_of_a_new_cyber_security_model/, accessed on March 12, 2015.