Responding a Cyber Catastrophe[1]

Among the 2014 trends, one significant topic is underlined, *Cyber Security*. Expansion of the use of internet globally, increasing dependency on IT for every aspect of life, growing concerns about privacy, ongoing covert/overt cyber operations and wars, cyber espionage activities are few reasons to underpin the importance. States are trying to develop defensive capacity, to build a deterrence in cyber space and to search for opportunities in order to improve their offensive or active defense capacity. In this manner, we are likely to be familiar with "cyber power capacity" and "cyber power indexes" in the upcoming years.

On the other hand, growing risks of intrusions into states' private, commercial and governmental networks and cyber-attacks having devastating consequences ignited the debates around new 9/11 but in cyber domain, *Cyber 9/11*. Many of the countries, defined cyber espionage and cyber-attacks against critical infrastructure as two national security threats in their cyber security strategy papers. Thus, public-private cooperation models, military preparedness, simulations, scenario-based events and model policy alternatives are published and prepared in order not to face a massive surprise cyber-attacks causes new 9/11,

Visualize a case in which a financial infrastructure collapsed, stock market was closed and financial transactions and banks came to a stop. Such kind of dire consequences, immediately drive society out, and create chaos. Even if there is not a traditional kinetic attack, well organized, complexly structured cyber weapons might be reason for that. Bearing in the mind this fictional scenario, providing resilience for the systems and preparedness for 9/11; policy alternatives and national-international, long term-short term response plans should be written. Cyber 9/12 Project[2], conducted by Atlantic Council's Cyber Statecraft Initiative in order to determine how transatlantic community would respond a cyber-catastrophe, is one of the good examples of it.

Hybrid cyber policy plans and responses

Proposing a response *the day after* massive surprise cyber-attack which leads dire consequences is important. In this regard, initially technical mitigation and recovery process have to be adopted. Incident management is key in this phase. It covers investigation, detection of malware, dynamic and behavioral malware analysis, containment and recovery. Furthermore, close cooperation with national and international authorities such as CERTs, ISPs and other service providers, international organizations like ICANN is important in this stage.

Secondly, diplomatic steps in which seeking an international cooperation and common international legal regimes become prominent. Implementing an effort to stimulate cooperation among *like-minded nations*[3] to produce common approaches, cyber norms and principles to deal with cyber espionage and cyber-attacks in a broader spectrum from disruptive to destructive paves the way for deterrence. Internationalization of the incident by calling international organizations like UN, OECD and regional organizations NATO, ASEAN, APEC etc., create a greater forum to raise awareness and intimidate similar potential attacks in the future.

---

[1] This analysis first appeared in Journal of Turkish Weekly on 18 February 2014.

[2] Jason Healey, *Preaparing for Cyber 9/12*, Atlantic Council Issue Brief, May 2012

[3] Franklin D. Kramer and Melanie J. Teplinsky, *Cybersecurity and Tailored Deterrence*, Atlantic Council Issue Brief, December 2013

Thirdly, keeping in the mind the legal and political consequences, defining the attack and its effects legally is critical. Whether cyber-attack can be defined as breach of sovereignty or use of force or armed attack depends on basically duration, intensity and what kind of consequences it leads (level of destruction, casualties etc.). Although defining the attack doesn't force us to give similar response, it specifies the spectrum of it. For example, any action overreaching the limits of armed attack give a targeted state an inherent right of self-defense. But state doesn't have respond similarly, it has the opportunity of responding in a large spectrum, economic sanctions, break diplomatic relations, countermeasures and retaliation. Further in case of an internationally wrongful act, breach of an international obligation, injured states may resort to proportionate countermeasures, including cyber and physical countermeasures. Moreover, the active cyber defense especially whether private sector has a right to retaliate, a natural privilege of states, or hack-back is another problematic issue likewise attribution.

To this end, *hybrid cyber policy and response models* are creative outcomes of *scenario-based models* in which they cover technical, diplomatic, political and legal aspects of the issue, considers national and international steps or responses separately, creates public-private cooperation in every phase of incident management and response phase, implements not only defensive but also offensive methods.