Centre for Economics
and Foreign Policy Studies

Cyber Governance and Digital Democracy 2017/4

December 2017

Chasing The Ghosts: Investigating The Attribution Of Transnational Cyber Attacks

Dr. Can Kasapoğlu | EDAM Defense Analyst

This paper was supported by
Robert Bosch Stiftung

Chasing The Ghosts: Investigating The Attribution Of Transnational Cyber Attacks

Dr. Can Kasapoğlu

> Cyber attacks fall under a misty and gray area which could be best depicted as ‘below the threshold of armed conflicts’, a hard-to-recognize hole within the margins of international law. Thus, cyber tools extraordinarily fit well with hybrid warfare and espionage purposes. Although the bulk of contemporary hostile cyber activities are related with state actors, these intrusions mostly take place in the form of proxy war which enables the states to keep being concealed in complex secrecy. In fact, high–end computer, network and telecommunications technologies help states to sustain the abovementioned ambiguity in their cyber operations.

Executive Summary

✓ Cyber attacks fall under a misty and gray area which could be best depicted as ‘below the threshold of armed conflicts’, a hard-to-recognize hole within the margins of international law. Thus, cyber tools extraordinarily fit well with hybrid warfare and espionage purposes. Although the bulk of contemporary hostile cyber activities are related with state actors, these intrusions mostly take place in the form of proxy war which enables the states to keep being concealed in complex secrecy. In fact, high–end computer, network and telecommunications technologies help states to sustain the abovementioned ambiguity in their cyber operations.

✓ Type, reliability and function of ‘evidences’, which are required to pursue a cyber investigation and conclude attribution, differ in a case by case fashion for states. Even various branches within a state’s security apparatus might develop their own approaches in evaluating cyber pieces of evidence. Nevertheless, almost the universal rule in cyber defense boils down to the very fact that there is a huge gap between technical and political attribution. Holding a state actor responsible for a cyber-attack is a complicated task. Furthermore, inaction or solely voicing a diplomatic rhetoric with no tangible steps following a precise political attribution may even hinder the deterrence capacity of the victim.

✓ Following a cyber intrusion, an investigation would have to prioritize one of the three main objectives, namely tracing back the attack to the immediate attackers, tracing back the attack to the computer systems from which the initial hostilities originated, or tracing back the attack to the mastermind / orchestrator state(s). Would precisely locating the attacker/computers necessarily mean a successful cyber investigation in the absence of a political context? This critical question could bring about different answers depending to a technical, political – military, legal, geopolitical, or strategic intelligence standpoint. Notably, multi – stage cyber attacks give a real boost to the aforementioned ambiguities.

✓ What could and should a state do following a successfully concluded cyber investigation which ended up with finding a clear suspect? This question necessitates a carefully framed assessment since responding to cyber attacks remains another key aspect of attribution. Skyrocketing offensive cyber know–how has already sparked the critical mass to deliver kinetic impacts. Moreover, the level of advancement and digitalization of critical infrastructure ironically make a nation more vulnerable to cyber hostilities. Therefore, modern state is in need of a roadmap when dealing with cyber attacks. In this regard, more energetic frameworks, first and foremost active cyber defense, come in to the picture. Yet, preventive and pre-emptive characteristics of these concepts inevitably cast doubts on their legality and potential benefits.

✓ Last but not least, even if active cyber defense – or lately responsive cyber defense – concepts could be put in practice, still, responding to cyber attacks would keep revolving around the very dilemma of what constitutes a legitimate target. At this point, the most critical factor remains the absence of norms regulating the cyberspace, let alone an international mechanism.

Centre for Economics
and Foreign Policy Studies

edam

Cyber Governance and Digital Democracy 2017/4

December 2017

Chasing The Ghosts: Investigating The Attribution Of Transnational Cyber Attacks

Dr. Can Kasapoğlu | EDAM Defense Analyst