Chapter 5

Threats to the Critical Information Infrastructure Protection (CIIP) Posed by Modern Terrorism

Metodi Hadji-Janev
International Relations and International Security Law, Republic of Macedonia

ABSTRACT

The emergence of new non-state actors in the post Cold War reality has dramatically changed security environment around the globe. Modern terrorism practiced by Al Qaeda and its associated movement (AQAM) has posed serious threat to critical information infrastructure given the trend of connecting control systems that run these infrastructures to the internet. Although AQAM have not been successful to launch a cyber-attack that will cause mass casualties, environment damage, or financial effects, the possibility remains alarming since creativity in the age of globalization never ends. Additionally, by using the so called “dot-com culture,” modern terrorists effectively employ negative effects of globalization to rich to the societies’ remote pockets and Islamic social nomads and thus enlarge their capabilities to affect our critical information infrastructure. Therefore, to effectively protect our CII from modern terrorists we need to consider comprehensive and holistic approach build on direct and indirect mechanisms.

INTRODUCTION

The end of the Cold War and technological development has stimulated the process of globalization. On one hand globalization has spurred economy and improved our way of living. On the other it has stimulated environment where non-state actors including terrorist organizations have gained unimagined power. Using violent ideology especially after military response to 9/11 attacks, Al Qaeda have build global network of associated movements. Launching an ideological war
these activists successfully have attracted many religious Islamic groups and individuals that were impressed with the idea to oppose.

Today Al Qaeda’s and its associated movements’ (AQAM) activities represent modern terrorism. They pose asymmetric, unconventional, and apocalyptic threats around the globe. In this context cyber-world has become both, battle-space for modern terrorists’ ideological and information warfare and medium for global radicalization.

AQAM’s interest to engage cyber-world for its own purposes raises serious alarm. Recent trend to connect control systems that run critical infrastructure to the internet makes these utilities especially vulnerable in the context of AQAM’s interest. Thus many modern systems that run our everyday life and we depend on are also infrastructures that could be used to affect our security. Yet until today AQAM have not been successful to launch large scale cyber-attack that will cause mass casualties, environment damage or financial effects. Nevertheless security analyses and recent practice confirm that AQAM can affect critical information infrastructure both directly and indirectly.

On one hand there are many open possibilities for AQAM to attack critical Information Infrastructure. Their leadership’s dedication to exploit internet, apocalyptic agenda and unconventional approach perfectly matches the possibility of threatening our CII. On the other, by using the so called “dot-com culture” modern terrorists effectively employ negative effects of globalization to rich to the societies’ remote pockets and Islamic social nomads. Although many of the AQAM’s supporters are second or even third generation Muslims (educated in West and raised surrounded by western values and culture), who have never met some of its leaders they have been radicalizes among other through internet. The practice (like in London attacks case for example) has shown that these self-radicalized individuals are equally or even more dangerous to detect and fight than the core AQAM cadre.

Therefore to effectively protect our critical information infrastructure and improve its resilience we need to consider comprehensive and holistic approach. This approach should include but is not limited to direct protective mechanisms like protective systems, supporting tools and technologies (with proper and timely updates), adequate and secure use of systems, general awareness of existing threats and appropriate security reporting. In addition indirect approaches that will reduce AQAM’s ability to influence support must be also considered if we are to improve our critical information infrastructure protection and its resilience.

1. PROCESS OF GLOBALIZATION AND THE SECURITY ENVIRONMENT AFTER THE COLD WAR

Influence of globalization and the emergence of new non-state actors in the post Cold War reality have dramatically changed security environment around the globe. This “Big Thing”-globalization as described by Friedman (2002) has become a driving force in international affairs (p xxi). Labeling it as a tectonic shift, Friedman describes globalization as an international system with its own rules and logic that influences the geopolitics and economics (p xxii). Despite the fact that globalization is largely associated with open markets and free trade many argue that globalization is technology driven.

Fukuyama (1992) claims that thanks to tecnology liberal democracies had grown sufficiently aware and interconnected to protect against cataclysmic warfare among superpowers, marking an end to the Cold War. Therefore he believes that the “expansion of globalization occurs most rapidly in lands that nurture the freedom of expression and enterprise” (p. 23-25). In this context Mead (2004), explains how “the glorious triumph of technology and entrepreneurial spirit over a decadent and stagnant era”, offer “new and more dynamic opportunities to eliminate poverty and
Related Content

A Decentralized Security Framework for Web-Based Social Networks  
[www.igi-global.com/article/decentralized-security-framework-web-based/2491?camid=4v1a](www.igi-global.com/article/decentralized-security-framework-web-based/2491?camid=4v1a)

Balanced Approach for Hiding Sensitive Association Rules in Data Sharing Environment  

A Proposed SOAP Model in WS-Security to Avoid Rewriting Attacks and Ensuring Secure Conversation  
[www.igi-global.com/article/a-proposed-soap-model-in-ws-security-to-avoid-rewriting-attacks-and-ensuring-secure-conversation/190858?camid=4v1a](www.igi-global.com/article/a-proposed-soap-model-in-ws-security-to-avoid-rewriting-attacks-and-ensuring-secure-conversation/190858?camid=4v1a)

Risk Assessment of Multi-Order Dependencies between Critical Information and Communication Infrastructures  
[www.igi-global.com/chapter/risk-assessment-multi-order-dependencies/74630?camid=4v1a](www.igi-global.com/chapter/risk-assessment-multi-order-dependencies/74630?camid=4v1a)