US Foreign Policy Challenges of Non-State Actors’ Cyber Terrorism against Critical Infrastructure

Natalia Tereshchenko, Russian Academy of Sciences, Moscow, Russia

ABSTRACT

What is cyber terrorism? The paper will examine how the fundamentalist interpretation of the Quran may affect the non-state actors’ terrorist approach to the cyber domain, the dangers of an assault and the possible side-effects in politics, international relations and the public domain. The author will approach the issue in political, legal and social terms, touching only slightly on issues such as espionage and inter-state relations. Examples of recent cyber attacks and probable future scenarios will be examined to produce a balanced US-oriented policy paper. Some problems are difficult to tackle and require time, skills and diplomacy, but this should not act as an abandonment of initiatives. Although the threat is not yet acute, it is worthwhile addressing at an early stage and preventing the vast harm that can be caused by cyber terrorism. Legislative and political initiatives should be advocated ensuring better cooperation and collaboration between parties.

Keywords: Critical Infrastructure, Cyber Terrorism, Epistemology, Fundamentalism, International Organizations, Jus Ad Bellum, Non-State Actors, Sun Tzu, United States (US) Foreign Policy

INTRODUCTION

Understanding why, how and with what consequences terrorists could and would want to use the cyber domain for their purposes is essential to formulating the best policy practices in preventing and managing the emergence of a cyber-empowered terrorist ‘community’. Discourse analysis, epistemology and Sun Tzu’s theory of war, along with other pertinent concepts of international relations provide a framework for looking at terrorists’ motivations and activities in the cyber world.

Technological developments have seen the virtual domain evolve dramatically, and the 21st century marked acceleration in both the online world and the threats that arise from it. The recent years have experiences not only an enhanced access to the internet worldwide, greater capabilities of programs and a wider range of ser-
vices. Computers have also brought technical, political, social and economic problems, with malware being born at a higher frequency than the cures for it. Controls over targets and over attackers have become exceedingly difficult to achieve; and in the latter—practically impossible. More elaborate and complex hacking tendencies often target critical objects—private and public. Although for now, cyber is a domain of close attention in inter-state relations, the potential for terrorist groupings developing the capabilities, access and the motivation to target State and, indeed, private infrastructure is very serious. Reports, research and intelligence information gathered suggest that in a couple of years from now, terrorists may acquire enough skills to use cyber space for attack purposes (GCN, 2012; Guneev, 2012).

The subject of cyber terrorism is situated within a new field of research; therefore specific publications are very limited. However, positioned in a wider context, research easily overlaps with many disciplines, and these will be explored in detail.

Authors, doctrines, governments and international organizations differ in opinion not only as to whether cyber terrorism is possible, but also as to the consequences of it, if taken as a plausible situation. Controversy in literature is largely based on the impossibility to define appropriately the terms and fit them into the existing legislation or into the policy of the state on cyberwarfare. Intelligence agencies and relevant actors are hesitant about giving any specific information on cyber terrorism. In recent sources they tend to agree that it poses a high threat. Yet, whilst FBI may look like it is in fear on the scale and proximity of such an attack (Albanesius, 2012; Camara, 2013; Hoover, 2012), NATO may at the same time be saying that this threat has not yet emerged to a full scale. They both confirm, nevertheless, that it is only a matter of months or a year that terrorists may acquire sufficient expertise to perform an attack in cyber space (Brewster, 2012). All agencies, government officials and the technical sector conclude that, as soon as terrorists get the sophistication, they will use it. In the very few years to come, says Eugene Kaspersky, we are likely to experience a cyber attack emanating from non-state actors and terrorists (Guneev, 2012; Bell, 2013).

What raises most discussions is the legality of response to cyber terrorism and how it fits into the law of war theory as a whole, if that is at all applicable.

Stewart Baker, the former Assistant Secretary for Policy under George W. Bush, believes that law puts unnecessary restrictions and acts as an impulse for disagreements on activities in cyberspace. When it is time to act to protect civilians and a nation, especially in offensive cyberwar, it may not be appropriate to look at the legality of the response. On the contrary, Charles Dunlap the former Deputy Judge Advocate General of the US Air Force, sees legal frameworks as indispensable and ethical—the absence of such may lead to war without limits. Dunlap also argues that it is not the absence of law per se that poses problems—it is the application of facts and complexities to the framework that renders judgements difficult (Dunlap, 2011, 2012).

Some, like Schmitt (1999) propose a new form of legislation, claiming that the existing one is insufficient to target the newly emerging threats. Prolific experts in the sphere, like Geers (2010a, 2010b) and Lewis (2010a), even suggest the adoption of a convention on arms control in cyberspace, which was discussed back in 2010, but never achieved a consensus (Homeland Security News Wire, 2010). Even internally, the recent attempt of the Congress to pass a new Cybersecurity Act has ended in a failure when the Republicans were reluctant to agree to the terms of the proposed Act, seeing it as governmental intrusion into businesses of private companies and into private lives overall (Levin, 2012; Vijayan 2012; Jaycox 2012). There have even been recent radical discussions on listing copyright infringement as cyber terrorism (Global Research, 2013).