ABSTRACT (EXTENDED VERSION)

HOW TO RESPOND TO EMERGING SECURITY THREATS IN CYBERSPACE: CHALLENGES AND OPPORTUNITIES

Suleyman Ozeren, Ph.D.
President of GLOBAL Policy and Strategy

Cyberterrorism and cybercrime present new challenges for law enforcement and policy makers. Due to its transnational nature, a real and sound response to such a threat requires international cooperation involving participation of all concerned parties in the international community. However, vulnerability emerges from increased reliance on technology, lack of legal measures, and lack of cooperation at the national and international level represents real obstacle toward effective response to these threats.

Over the past several years, terrorism has been one of the complex issues faced by government policy makers, analysts, and the public. The complexity of terrorism has emerged not only from the definition of the concept itself but also the tactics that terrorist groups use, the countries that support terrorist groups, and the policies and procedures that have been used to counter terrorist actions by the target countries.

Terrorists and cyber criminals will exploit vulnerabilities, including technical, legal, political, and cultural. Such a broad range of vulnerabilities can be dealt with by comprehensive cooperation which requires efforts both at the national and international level.

The information age is shaping not only the types of weapons and targets the terrorists select, but also the ways that terrorist groups structure and operate their organizations (Zanini and Edwards, 2001, p. 30). According to Zanini and Edwards, large terrorist organizations are using information technologies, such as computers, telecommunication devices, software, and the Internet to organize and coordinate activities (2001, p. 30).

Criminality originating from new technologies, such as the Internet, wireless communications, and other computer networks creates many challenges for law enforcement around the world (Sussmann 2000). Responding to cyberterrorism and investigating computer-related crimes pose challenges for law enforcement, as well as the legal system.

Terrorist groups are effective agents in public cyberspace and online propaganda is a common method that terrorist organizations use to attract and recruit potential members. It allows militants to take advantage of the ease and the convenience brought about by the improvements in communication technologies and enables them to reach to and motivate their sympathizers.

Among many other media tools, online communication instruments and the public cyberspace generated by these instruments are the foremost agents of construction for individuals’, groups’, movements’, and institutions’ meaning and identity. Particularly, social media platforms like Twitter, YouTube, Facebook and many others highly mediate this construction process and allow individuals to communicate without dependence on traditional organizational hierarchies.
There is a positive relationship between vulnerability and comprehensive cooperation; in other words, higher vulnerability requires a higher level of cooperation. Therefore, developed countries, in particular, those that are under threat of cybercrime and cyberterrorism or traditional terrorism should seek more cooperation with other countries.

Cooperation is very critical in terms of responding to cyberterrorism and cybercrime. Cooperation at the national level includes law enforcement and private sector. Sometimes overlaps in terms of the responsibilities and authorities between different law enforcement agencies may cause confusion. To avoid such an event, law enforcement should establish a coordination center that will not be a supervisory unit, but a unit which will facilitate coordination and collaboration between layers of bureaucracy.

Secondly increasing awareness of vulnerabilities to cyberterrorism and cybercrime can be facilitated by training of law enforcement and the public.

Third, the international cooperation factor represents one of the major aspects of this research. While there are numerous issues regarding how to achieve a sound international cooperation, the first step toward it involves believing in establishing international cooperation. In other words, countries should spend time and energy establishing a general consensus as to what they should do to achieve real cooperation.

To achieve a real cooperation at the international level, countries should practice real coordination and exchange of intelligence. Formal bilateral and multilateral agreements and organizations achieve some level of cooperation, but bureaucracy and other obstacles may slow down the procedures which are very critical in investigating cybercrime. To solve that problem, countries should look for ways to practice informal cooperation at least among the law enforcement agencies.

Moreover, legal measures play a very critical role in responding to cybercrime and cyberterrorism.

Finally, we need to find out new strategies and tactics to respond to the overwhelming problems we face today. Global nature of the issues such as cybercrime and terrorism requires global responses. It is necessary to look for a radical approach. Globalization of crime, in fact, asks for globalization of law enforcement. This statement may sound overambitious; however, given the extent and complexity of cybercrime and terrorism, it may be underestimating the seriousness of these problems if we claim otherwise.
HOW TO RESPOND TO EMERGING SECURITY THREATS IN CYBERSPACE: CHALLENGES AND OPPORTUNITIES

Suleyman Ozeren, Ph. D.
Introduction

Understanding the phenomenon

Technology and terrorism

Cyberterrorism Typology

The CFRP Factor

The concept of vulnerability

International cooperation

Global Response

Analysis

Discussions and Conclusion
I tried cyber crime, but I prefer people-to-people contact."
Terrorism as a Concept

- Defining the concept
- Labeling or frameworking issues
- Lack of consensus
- Terrorism as a “communication strategy”

Some of the Major Components of Counterterrorism

- Diplomacy
- Legal measures
- Financial control
- Prevention
- Offensive force (Police and military)
- Intelligence
Emerging Threats of Cyberterrorism

The convergence of terrorism and cyberspace.

- Cyberterrorism and cybercrime present new challenges for law enforcement and policy makers.
- Due to its transnational nature, a real and sound response to such a threat requires international cooperation involving participation of all concerned parties in the international community.
- Over the past several years, terrorism has been one of the complex issues faced by government policy makers, analysts, and the public.
- The complexity of terrorism has emerged not only from the definition of the concept itself but also the tactics that terrorist groups use, the countries that support terrorist groups, and the policies and procedures that have been used to counter terrorist actions by the target countries.
- Terrorists and cyber criminals will exploit vulnerabilities, including technical, legal, political, and cultural.
- Such a broad range of vulnerabilities can be dealt with by comprehensive cooperation which requires efforts both at the national and international level.
The information age is shaping not only the types of weapons and targets the terrorists select, but also the ways that terrorist groups structure and operate their organizations (Zanini and Edwards, 2001, p. 30).

According to Zanini and Edwards, large terrorist organizations are using information technologies, such as computers, telecommunication devices, software, and the Internet to organize and coordinate activities (2001, p. 30).

Criminality originating from new technologies, such as the Internet, wireless communications, and other computer networks creates many challenges for law enforcement around the world (Sussmann 2000).

Responding to cyberterrorism and investigating computer-related crimes pose challenges for law enforcement, as well as the legal system.
Emerging Threats of Cyberterrorism III

- Terrorist groups are effective agents in public cyberspace and online propaganda is a common method that terrorist organizations use to attract and recruit potential members.

- It allows militants to take advantage of the ease and the convenience brought about by the improvements in communication technologies and enables them to reach to and motivate their sympathizers.

- Particularly, social media platforms like Twitter, YouTube, Facebook and many others highly mediate this construction process and allow individuals to communicate without dependence on traditional organizational hierarchies.
The Concept of Cyberterrorism

The convergence of terrorism and cyberspace.

It is generally understood to mean unlawful attacks and threats of attacks against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political and social objectives.
## Category of Cyberterrorism

<table>
<thead>
<tr>
<th>Category</th>
<th>Definition and Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information attacks</td>
<td>Cyber terrorist attacks focused on altering or destroying the content of electronic files, computer systems, or the various materials therein.</td>
</tr>
<tr>
<td>Infrastructure attacks</td>
<td>Cyberterrorist attacks designed to disrupt or destroy the actual hardware, operating platform, or programming in a computerized environment.</td>
</tr>
<tr>
<td>Technological facilitation</td>
<td>Use of cyber communications to send plans for terrorist attacks, incite attacks, or otherwise facilitate traditional terrorism or cyberterrorism.</td>
</tr>
<tr>
<td>Fund raising and promotion</td>
<td>Use of the Internet to raise funds for a violent political cause to advance an organization supportive of violent political action, or to promote an alternative ideology that is violent in orientation.</td>
</tr>
<tr>
<td>Cyberterrorism Typology</td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Disruptive and destructive information attacks</strong></td>
<td><strong>Facilitation of technology to support the ideology</strong></td>
</tr>
<tr>
<td>Unauthorized Access</td>
<td>Money Laundering</td>
</tr>
<tr>
<td>Virus</td>
<td>Fraud</td>
</tr>
<tr>
<td>Denial Of Service Attack</td>
<td>ID Theft</td>
</tr>
<tr>
<td>Tampering Data</td>
<td>Forgery</td>
</tr>
<tr>
<td>Trojan</td>
<td></td>
</tr>
<tr>
<td>Espionage</td>
<td></td>
</tr>
<tr>
<td>Worms</td>
<td></td>
</tr>
</tbody>
</table>
TYPOLGY OF CYBETERRORISM

Information attacks

Defacing Web sites

Malicious Code Attacks – Malware
Viruses
Worms
Trojan horses

Denial of Service Attacks
Message Flooding
Signal Grounding
Infrastructure Attacks

Attacks against critical infrastructures

Disruptive attacks

In 1992, Chevron’s emergency alert network disabled the firm’s alert system by hacking into computers in New York and San Jose, California.
Technological Facilitation

The use of advanced technology in terms of computers and telecommunication devices enables terrorist organizations to operate with greater flexibility, and shapes their organizational structure toward more decentralized structure.

Information technologies are very advantageous for dispersed groups and may, if not totally, eliminate the disadvantages of created by distance.
The Internet

It provides extremely effective communication between the terrorist organization and its members.

Eight different ways that terrorists use the Internet:

• Psychological warfare,
• Publicity and propaganda,
• Data mining,
• Fundraising,
• Recruitment and mobilization,
• Networking, sharing information, and
• Planning and coordination.
**THE CONCEPT OF VULNERABILITY**

Definition: a weakness in system security procedures, system design, implementation, internal controls, etc., that could be exploited to violate the system’s security policy.

4 types of vulnerabilities are identified by the researcher:

1. Technical aspects of vulnerability
2. Legal aspects of vulnerability
3. Political aspects of vulnerability
4. Cultural aspects of vulnerability
Two factors are very important

**First**, whether there are targets that are vulnerable to attacks that could lead to severe harm, and

**Second**, whether there are actors with capability and motivation to carry them out”.
Vulnerability (Conceptual Definition):

Vulnerability is defined as

- any weakness stemming from any loophole in a system security, lack of awareness of potential attacks,

- lack of legal systems criminalizing any action against critical information infrastructures, presence of terrorist groups which may have motivation and capability of cyber attacks,

- and lack of cooperation and coordination among the law enforcement entities and between the public and private sectors.
International Cooperation refers to any bilateral or multilateral agreements made and/or ratified by a country to facilitate cooperation with another country or international/supranational organization to respond to crime involving cybercrime and cyberterrorism.
INTERNATIONAL COOPERATION
GLOBAL RESPONSE

- A common terminology between parties involved in the incident to include identification of the intruder’s modus operandi, the technical attack details, and the identification of the targets,

- Knowledge of the technical skills of all parties involved in resolving the incident

- Existing agreements on how incidents of a variety of types will be handled

- An understanding of the common and conflicting societal issues surrounding the incidents.
GLOBAL RESPONSE

➢ Broad membership, consisting of both the world’s most technologically advanced nations as well as developing nations, all of whom share the benefits and the risks of global information

➢ A voluntary and non-coercive environment based on concepts of consensus and practical experience

➢ Open technical standards that prevent the manipulation of information technology for unilateral gain

➢ An open organizational structure that provides opportunities for all constituencies to express their concerns
GLOBAL RESPONSE

- A mechanism for providing continuous monitoring of actions that can adversely impact privacy

- Mechanisms for reviewing the state of information technology and its practical implementations to enable the international framework to remain relevant in the light of changing capabilities and requirements

- Mechanisms that can assist in building trust relationships globally

- Funding arrangements that can assist less developed nations in meeting their responsibilities to protect the information commons.
GLOBAL RESPONSE

- Formal bilateral cooperation: Mutual Legal Assistance Treaties (MLATs)
- Informal bilateral cooperation: Individual police contacts (inter agency cooperation), etc.
- Formal multilateral cooperation: Council of Europe
- Informal multilateral cooperation: G-8 OECD, APEC, CERT collectives.
<table>
<thead>
<tr>
<th>International Level of Cooperation</th>
</tr>
</thead>
<tbody>
<tr>
<td>➢ United Nations</td>
</tr>
<tr>
<td>➢ Group of 8:</td>
</tr>
<tr>
<td>➢ Council of Europe</td>
</tr>
<tr>
<td>➢ European Union</td>
</tr>
<tr>
<td>➢ Asia-Pacific Economic Cooperation (APEC)</td>
</tr>
<tr>
<td>➢ Organization for Economic Cooperation and Development (OECD)</td>
</tr>
<tr>
<td>➢ Interpol</td>
</tr>
<tr>
<td>➢ European Police Office (Europol)</td>
</tr>
</tbody>
</table>
The research shows that there could be a variation of vulnerability among countries which may have the same level development in terms of reliance on technology and other things that make those countries more vulnerable.

Reliance on technology may be a source of vulnerability, but implementation of security measures may decrease the risk of being a target of an unfortunately successful attack.
LIMITATIONS

✓ The difficulty emerges from obstacles to investigate and prosecute such crimes due to the nature of the crime itself.

✓ The unwillingness of the victims of these attacks to report their victimization.

✓ Secrecy

✓ Supranational Entities

✓ The specific expertise of the individuals may affect their responses which may make it difficult to establish a common ground.
OBSTACLES IMPACTING INTERNATIONAL COOPERATION

- Lack of adequate laws defining terrorism
- Lack of well-defined and structured practices and patterns of cooperation
- National sovereignty and sensitivity over international cooperation
- Lack of consensus and adequate laws defining terrorism
DISCUSSION

✓ International cooperation factor is as complex as the domestic level of cooperation if not more.

✓ Issues of sovereignty and national security.

✓ Foreign policy issues – National interest

✓ Difficulty to establish a general consensus
SOME RECOMMENDATIONS I

- The international cooperation factor represents one of the major aspects of this research. While there are numerous issues regarding how to achieve a sound international cooperation, the first step toward it involves believing in establishing international cooperation.

- In other words, countries should spend time and energy establishing a general consensus as to what they should do to achieve real cooperation. Based on the research results, while multilateral cooperation is desirable, bilateral agreements are considered as more achievable than multilateral agreements.

- Therefore, countries should focus on establishing more bilateral agreements with other countries; they also should explore new venues to set up multilateral cooperation.

- To achieve a real cooperation at the international level, countries should practice real coordination and exchange of intelligence.

- Formal bilateral and multilateral agreements and organizations achieve some level of cooperation, but bureaucracy and other obstacles may slow down the procedures which are very critical in investigating cybercrime.

- To solve that problem, countries should look for ways to practice informal cooperation at least among the law enforcement agencies.
Moreover, legal measures play a very critical role in responding to cybercrime and cyberterrorism. The laws and conventions, such as the Council of Europe Convention on Cybercrime are useful tools to facilitate cooperation.

In order to respond to transnational crime, such as cybercrime and terrorism, having a common definition of the crime is vital.

Recognizing the importance of defining a crime according to its unique characteristics will not only ease the investigation procedures, but also enable cooperation with other countries.

Therefore, countries should reattempt to come up with internationally accepted definitions of terrorism, cybercrime, and cyberterrorism.
Finally, we need to find out new strategies and tactics to respond to the overwhelming problems we face today.

Global nature of the issues such as cybercrime and terrorism requires global responses.

It is necessary to look for a radical approach. Globalization of crime, in fact, asks for globalization of law enforcement.

This statement may sound overambitious; however, given the extent and complexity of cybercrime and terrorism, it may be underestimating the seriousness of these problems if we claim otherwise.
THANK YOU FOR YOUR ATTENTION

Suleyman OZEREN, Ph. D.

GLOBAL Policy and Strategy Institute
http://www.globalpse.org