Vol.3 • No.2 • Fall 2010

ISSN. 1307-9190

CENTRE OF EXCELLENCE - DEFENCE AGAINST TERRORISM
2004
TURKEY

Defence Against Terrorism Review

DATR

Gábor IKLÓDY
The New Strategic Concept and the Fight Against Terrorism: Challenges & Opportunities

Jaak AAVIKSOO
Cyberattacks Against Estonia Raised Awareness of Cyberthreats

Alan E. BRILL
From Hit and Run to Invade and Stay: How Cyberterrorists Could Be Living Inside Your Systems

Marco GERCKE
Challenges in Developing a Legal Response to Terrorist Use of the Internet

Anna-Maria TALİHÄRM
Cyberterrorism: in Theory or in Practice?

Julian CHARVAT
Radicalization on the Internet

Centre of Excellence-Defence Against Terrorism

COE-DAT

Defence Against Terrorism Review - DATR

Owner
COE–DAT

Co-ordinator
Col. Özden Çelik, Chief of the Education and Training Dept., COE–DAT

The views presented are those of the authors and do not reflect or represent the views of the editors or the Centre of Excellence-Defence Against Terrorism

Defence Against Terrorism Review
DATR

Vol. 3, No. 2, Fall 2010

ISSN. 1307-9190

CONTENT

Editor's Note,

The Fall of 2010 witnessed intense debates in the international arena on various platforms, extending from academic institutions to international organizations, on future threats to international security and stability. A number of emerging threats have been noted with a high degree of caution by academics, politicians, and diplomats, as well as by civilian and military experts. The most important of which, from our perspective, being the variety of threats posed by the recent developments in cyberspace. At the Lisbon Summit of the North Atlantic Treaty Organization (NATO) in November 2010, the Heads of States and Governments adopted a new Strategic Concept that clearly highlighted terrorism as one of the enduring security challenges for the Alliance, with concerns about terrorism in cyberspace being a key issue. With these thoughts in mind, we decided to dedicate this issue to cover the various dimensions of the threats emanating from the advancements in the field of Information Technologies (IT).

The first article by Assistant Secretary-General of NATO, Ambassador Gabor Iklody, entitled "*The New Strategic Concept and the Fight Against Terrorism: Challenges and Opportunities*" argues that the multifaceted nature of the terrorism threat demands comprehensive countermeasures and multi-layered cooperation, especially in the area of prevention. Hence, the article elaborates the current role of NATO in the fight against terrorism and provides insights into the many opportunities and challenges that lie ahead in combating terrorism and its interrelated emerging security challenges following the adoption of the new Strategic Concept document by the Alliance.

As a more specific example of the damages that may be incurred by attacks in cyberspace, the article by Mr. Jaak Aaviksoo, Minister of Education and Research of Estonia, in his article, entitled "*Lessons Learned from the Cyber Attacks in April 2007*" contains important information as well as lessons to be drawn in these respects. The article argues that growing cybersecurity problems are the fact of the irreversible and irresistible movement toward an ever more interconnected and information-based world. Noting that in April 2007, Estonia experienced a coordinated and massive attack against government infrastructure, financial service providers and domestic media, Estonian authorities have realized that the old dividing lines between domestic and international conflicts, defense and security problems, law enforcement and military solutions, and public and private issues do not hold in cyberspace. Hence, Mr. Aaviksoo advances a new concept that he calls "the notion of good cybercitizenship," believing it crucial that a precondition for securing cyberspace is that every owner of a computer, computer network or information system feels responsible for the expedient and prudent use of information and communications technology.

The third article by Alan E. Brill, Senior Managing Director, Secure Information Services, Kroll, Inc., in his article entitled "*From Hit and Run to Invade and Stay: How Cyberterrorists Could Be Living Inside Your Systems*" presents the many facets of cyberattacks, including new tactics, such as hit-and-run to gain and maintain long-term access to the digital infrastructure of the enemies, as well as the tools of cyber-invasions that can be used to prepare to disrupt or disable technology based targets, ranging from factories to military communication systems. Mr. Brill describes the evolution of the threat, and suggests ways to meet the challenges posed by the Advanced Persistent Threat (APT) scenario, suggesting a number of defensive measures to consider when arguing that the selection of the right measures for use in a particular situation must flow from the sensitivity of the data, the likelihood that it will be targeted, and the architecture of the network and physical environment within which it is running.

Dr. Marco Gercke, Director of the Cybercrime Research Institute at the University of Cologne in Germany, in his article entitled "*Challenges in Developing a Legal Response to Terrorist Use of the Internet*" elaborates on the difficulties in investigating and preventing cybercrime in general and the terrorist use of the Internet in particular from a legal perspective. Dr. Gercke argues that the network technology in place addresses technical demands, which are not necessary in line with the priorities of the authorities involved in the fight against terrorist use of the Internet. Despite the fact that the legal community has started to address the problem of terrorist use of the Internet, either through specifically targeted legislation, or new uses of broader criminal legislation, Dr. Gercke concludes that there are still significant gaps in the legal framework that need to be addressed, and suggests that national provisions must be closer to one another for easier and more effective fight against cybercrimes and the terrorist use of the Internet.

Anna-Maria Talihärm from NATO Cooperative Cyber Defence Centre of Excellence in Estonia, in her article entitled "*Cyber Terrorism: in Theory or in Practice?*" emphasizes that in the absence of a commonly accepted interpretation, cyberterrorism is frequently discussed in media, politics, and security reports with great inconsistency regarding the meaning of the concept. Hence, she argues that the term has been used to describe virtually everything from simple hacking to fatal cyberattacks causing serious financial harm and bloodshed. In the same vein, the terminological confusion accompanying the debates over cyberterrorism has raised the question of whether it is feasible or at all possible to clearly define an incident that may not have taken place. In this respect, Talihärm's article is an attempt to define cyberterrorism by examining the different aspects of determining the meaning of the term as well as underlining the commonly supported target-oriented approach. The author concludes that using the term 'cyberterrorism' to describe current cyberincidents should be put on hold until the facts of the case can be matched with the combination of political and social motivation, serious damage, and fear.

Finally, Major Julian Charvat from COE-DAT touches upon a very sensitive topic, which is also the title of his article on "*Radicalization on the Internet,*" where he looks at how and why some people are vulnerable in society and targeted by terrorist organizations in an attempt to recruit them. Major Charvat argues that the issue of radicalization is one that affects all terrorist groups and that it is not just a religious issue but also the process that draws someone from being a passive supporter of a view to being an active foot soldier as a terrorist. Hence, the process can be gradual or instantaneous and will be impacted by the life experience of the individual. The author suggests that whatever the reasons people have for becoming more radical, it is important that this process be thoroughly understood in order to find a way of combating it and that it is vital to listen to what is being said by those trying to radicalize others and how it is being said. He concludes that those engaged in the fight against terrorism must understand what message is being said and how the target population is accessing it.

With so many expert opinions presented in a one single issue of our journal on the subject of criminal and/or terrorist uses of the cyberspace, we believe that a wide array of our readership will be able to amplify their knowledge and understanding of the dimensions of a major problem area in the study of international terrorism. It goes without saying that this subject needs much more elaboration in various platforms and venues in order to effectively deal with the threats ahead.

Mustafa Kibaroğlu,

Editor-in-Chief

Defence Against Terrorism Review
Vol.3, No. 2, Fall 2010, pp. 3-12
Copyright © COE-DAT
ISSN: 1307-9190

The New Strategic Concept and the Fight Against Terrorism: Challenges & Opportunities

Ambassador Gábor IKLÓDY
Assistant Secretary - General, NATO Headquarters, Brussels, Belgium

Abstract: *Terrorism is an enduring challenge to international security and stability. In the beginning of the 21st century, the terrorism threat environment has continuously evolved to become more complex and diffuse. It is therefore unlikely that international terrorism will become less of a threat in the coming years. The multi-faceted nature of the terrorism threat demands comprehensive countermeasures and multi-layered cooperation, especially in the area of prevention. This article will elaborate on the current role of NATO in the fight against terrorism and will provide insights into the many opportunities and challenges that lie ahead for the Alliance in combating terrorism and interrelated emerging security challenges following the adoption of the new Strategic Concept.*

Keywords: *Terrorism, International Security, Cyberattack, WMD, Organized Crime*

Introduction

At their November 2010 Lisbon Summit, the NATO Heads of States and Governments adopted a new Strategic Concept[1] that clearly highlights terrorism as one of the enduring security challenges for the Alliance. In the Alliance's 1999 Strategic Concept, terrorism was identified essentially as a risk affecting NATO's security. With the adoption of the new Strategic Concept, the Alliance decided to "enhance the capacity to detect and defend against international terrorism, including through enhanced analysis of the threat, more consultations with our partners, and the development of appropriate military capabilities, including help to train local forces to fight terrorism themselves."

[1] Strategic Concept for the Defence and Security of the Members of the NATO, 2010

In addition to the Strategic Concept, the Lisbon Summit Declaration stated clearly that NATO will "continue to enhance both the political and military aspects of NATO's contribution to deter, defend, disrupt and protect against [terrorism] including through advanced technologies and greater information and intelligence sharing. We reiterate our continued commitment to dialogue and practical cooperation with our partners in this important area."

The Lisbon Summit was a watershed for the Alliance, as it indicated that emerging security challenges – cyber, energy, proliferation and terrorism – were moving from the periphery towards the centre of the Alliance's agenda.

The new Strategic Concept lays the groundwork for an Alliance that responds to an increasingly globalized and more complex security environment by becoming more ***effective, efficient and engaged***. More *effective*, because NATO will invest in key capabilities such as Missile Defence and the protection of information systems. More *efficient*, because NATO is cutting old fat while building new muscle by transforming itself from a mainly defence Alliance into a multi-faceted security organization. Through investments in *smart defence*, NATO will have the capacity and the capabilities to deal with multiple threats simultaneously. In the area of counterterrorism, the Alliance will take a holistic approach to address these inter-related and non-traditional threats stemming from the proliferation of WMD, critical infrastructure, cyber attacks, and piracy. In such a threat environment, the promotion of the Alliance's security is thus best assured through a wide network of partner relationships with countries and organizations around the globe. Therefore, the Alliance will become more *engaged* by deepening existing partnerships and reaching out to new partners around the globe, as well as other International Organizations.

The Evolving Terrorism Threat Environment[2]

In the NATO Glossary of Terms and Definitions of the NATO Standardization Agency, (1989) terrorism is defined as the unlawful use or threatened use of force or violence against individuals or property in an attempt to coerce or intimidate governments or societies to achieve political, religious or ideological objectives.

Terrorism as an illegal tool, method, process and projection of psychological and physical violence presents a continuing threat to the international community.[3] Ten years after the attacks of September 11, the terrorism threat has not diminished as an international security challenge. Instead, the threat posed by terrorism has become increasingly complex and diffuse. As the Strategic Concept underlines, "Terrorism poses a direct threat to the security of the citizens of NATO countries, and to international stability and prosperity more broadly. Extremist groups continue to spread to, and in, areas of strategic importance to the Alliance, and modern technologies increase the threat and potential impact of terrorist attacks, in particular if terrorists were to acquire nuclear, chemical,

[2] Please note that while national terrorist groups are of great concern, the fight against international terrorism will be the focus of this article.

[3] Alexander, Yonah, "Contemporary Terrorism: From National to Regional and Global Threats", in Defence Against Terrorism Review, Vol. 1, No. 2, Fall 2008, pp. 41-46

biological or radiological capabilities."[4] Terrorism reveals new trends and dangers given its capacity for rapid and continuous evolution. First, due to the effects of globalization and increased, the security environment is increasingly affected by hybrid threats. Terrorism intersects with other emerging security challenges, for instance cyber threats, proliferation of Weapons of Mass Destruction, illegal transnational activities such as trafficking in arms, people and narcotics as well as with critical infrastructure protection, maritime, airspace and air transport security. Second, instability or conflict beyond NATO's borders can foster extremism, terrorism, and transnational illegal activities such as trafficking in arms, narcotics and people. Other factors contributing to the spread of terrorism could be the absence of socio-economic opportunities and the lack of democratic structures. Third, on an international level, Al-Qa'ida (AQ) is still very much in existence and a decentralized network of franchises and affiliates such as AQ in Iraq (AQ-I), AQ in the Islamic Maghreb (AQIM) and AQ in the Arabian Peninsula (AQAP) has become increasingly challenging. Fourth, the spread of modern means of communication, primarily the Internet, has played an important role in the increase of home-grown terrorism. Terrorists use increasingly sophisticated means of propaganda to reach out to potential recruits worldwide.

While "the meaning of the term has changed so frequently over the past decades,"[5] there is no common definition that describes the evolving threat in its entirety.[6] A number of common criteria can be found, however. Terrorists are non-state actors that pursue certain political and/or ideological objectives. For example, AQAP's stated goal is to cleanse the Arabian Peninsula of foreign influence, particularly from Western military personnel and civilian contractors and to establish a single Islamic caliphate in place of the existing regimes in Yemen, Saudi Arabia and the Gulf. Through international networks, terrorist groups thrive on collaboration across national boundaries often on the basis of broadly shared ideologies and commitment. Looking at AQ Central and its affiliates, the connection is often based on personal relationships, primarily ideological and often publicly declared for media effects. With regard to means, terrorists use tactical-level methods, such as modern communications tools, and a broad range of conventional weapons, among them improvised explosive devices, for their strategic-level objectives in order to impact policies of governments and the minds of populations. In general, terrorist groups follow a pattern that is comprised of recruitment, networking, targeting and attack. Furthermore, near-miss operations may be sufficient for terrorists to get their message across and intimidate an audience larger than the immediate victims of the attack. In addition, such operations can force the intended target to adopt expensive countermeasures which can be almost as large an expenditure as after a successful attack. The repercussions of the attacks in the United States in 2001, in Spain in 2004 and in the United Kingdom in 2005 could be felt on a global scale. Responding to the threat posed by terrorism, governments tend to improve intelligence sharing, to introduce legal and financial measures

[4] Strategic Concept for the Defence and Security of the Members of the NATO, 2010.

[5] Hoffman, Bruce, "Inside Terrorism", 2006, p. 3

[6] The EU defines as terrorism those acts that, given their natural context, may seriously damage a country or an International Organization, and that are committed with the aim of seriously intimidating a population and duly compelling a government or international organization to perform any act. Seriously destabilizing or destroying the fundamental political, constitutional economic or social structures of a country or an international organization is to be defined as terrorism.

and to tighten security controls, primarily in mass transport systems or public places. While the general public and governments consider these measures necessary, they also tend to reinforce the psychological threat posed by terrorism. The high costs associated with such measures and the widespread fear of terrorism can be easily exploited by terrorist groups. In October 2010, the United States, the United Kingdom and Saudi Arabia cooperated to uncover two bombs hidden in printer-ink cartridges destined for the United States on airlines en route with Fed Ex and UPS cargo firms. As a result, discussions emerged among Western States about the necessity to enhance controls from currently 5% to approximately 90% of all cargo packages. As such measures would lead to a tremendous increase in costs, AQAP issued a statement saying that even though the bombs had not reached their destination, the success of the near-miss attack was clearly visible given the additional economic costs Western States were now bearing to counter terrorism. Disproportionate responses to terrorist attacks, especially military responses, also bear a high risk of backfiring because of the diffuse threat posed by terrorism and the difficulty to eradicate terrorism even locally or deter it by sophisticated military means.[7]

Emerging Security Challenges and Terrorism

The terrorist group Al-Qa'ida in the Arabian Peninsula (AQAP) has increasingly targeted energy infrastructure. Al-Qa'ida Central, in turn, has been actively pursuing Weapons of Mass Destruction. Evidently, terrorism has become increasingly intertwined with other security challenges leading to an environment that is more diverse, rapidly evolving and unpredictable. Some of the key themes in this evolution are briefly summarized in the following section.

Energy Security / Critical Infrastructure Protection and Maritime Security

In the coming years, a return to global economic growth as well as the impact of natural disasters, such as the Japanese earthquake, will continue to put pressure on a number of highly strategic resources, including energy. In light of rising energy demands the availability, reliability, and affordability of energy supplies, the so-called geopolitics of energy, are becoming increasingly important to states. Disrupting energy production and transit are therefore becoming more and more attractive to terrorists and pirates. AQ affiliates in Iraq and Yemen continue to attack energy facilities and supply routes. In Iraq, the Government stated that it needs to increase the number of its 40,000 men strong oil police by 30% in order to protect its oil facilities from terrorist attacks. The protection of energy pipelines, facilities, and shipping from terrorist attacks is therefore a key security concern.

With regard to maritime security, including Sea Lanes of Communication (SLOCs), bottlenecks like the Strait of Malacca and harbor protection, the expansion of violence through the proliferation of piracy and terrorism is another cause for concern. Terrorist groups have conducted multiple attacks in open waters. AQ has demonstrated its reach through high-visibility attacks on the *USS Cole* and the *MV Limburg*. With regard to piracy, the United Nations estimates the annual costs in the Indian Ocean to be between $5 billion and $7 billion. While pirates are not regarded as terrorists, connections between AQ-affiliates and the Somali pirates are of growing concern.

[7] Lemann, Nicholas, "Terrorism Studies - Social scientists Do Counterinsurgency," New Yorker - 26 April 2010.

Use of Internet and Cyber Attacks

There are multiple ways for terrorists to use information technology to reach their objectives. Terrorists use the Internet as the most effective communication tool around the globe. They exploit the web to indoctrinate and radicalize followers, to gather information for plotting and planning new attacks, or to identify and train like-minded individuals. Therefore, access to the Internet has become increasingly important for terrorists and their supporters. Apart from the operational use of the Internet, terrorists could also attack information networks or computer systems by conducting cyberattacks. Currently, it is estimated that terrorists do not have the means yet to conduct large-scale cyberattacks. As technology is evolving, however, the terrorist threat to cyber space is also increasing. A terrorist threat could stem from the development and use of a web-based attack strategy aimed at critical infrastructure and information systems. Given the disruptive potential of such an attack, cyber terrorism would fit well into the strategic-level objectives of terrorists.

Weapons of Mass Destruction (WMD)

President Obama stated that "If an organization like Al-Qa'ida got a weapon of mass destruction on its hands — a nuclear or a chemical or a biological weapon — and they used it in a city, whether it's in Shanghai or New York, just a few individuals could potentially kill tens of thousands of people, maybe hundreds of thousands."[8] Al-Qa'ida's long-standing interest in acquiring WMD is well known. As Graham Allison points out in "Al-Qa'ida Weapons of Mass Destruction Threat: Hype or Reality?,"[9] Osama Bin Laden assigned members of his network to different tasks in the overall effort of the group to acquire WMD. In order to increase the probability of success of the entire operation, these members were assigned to act and report independently. Furthermore, AQ joined efforts with other terrorist groups, demonstrating that the interest and the motivation to possess WMD goes beyond Bin Laden's network. So far, the efforts of terrorist groups to acquire or use these weapons have not been successful. A 2008 bipartisan report of the United States' Commission on the Prevention of WMD Proliferation and Terrorism however asserts that it is likely that terrorists will resort to biological attacks by 2013 if governments fail to undertake major security and preventive measures. For the near future, militant groups may be able to deploy crude CBRN weapons, so-called "dirty bombs," which are also referred to as "weapons of mass disruption." Such weapons would cause limited destruction, but would certainly create panic and fear and could lead to major economic disruption. However, even if the use of WMD remains confined to the high end of the threat spectrum, in the words of Harold Agnew,[10] "If you believe that it is easy to make an improvised nuclear weapon, you are wrong. But if you believe it is impossible for a terrorist group to make an improvised nuclear bomb, you are dead."

[8] Remarks by President Barack Obama at Town Hall Meeting with Future Chinese Leaders, The White House, Office of the Press Secretary, 2009.

[9] Mowatt-Larssen, Rolf, "Al-Qa'ida Weapons of Mass Destruction Threat: Hype or Reality? A Timeline of Terrorists' Efforts to Acquire WMD," Belfer Center for Science and International Affairs, 2010.

[10] Harold M. Agnew, a nuclear weapons engineer, became the third US Los Alamos National Laboratory Director in 1970. He also served as Scientific Advisor to NATO.

Nexus with Organized Crime and Narcotics

Weak states can directly threaten international security and stability through the state's inability to secure its territory, providing opportunities for terrorists to create safe havens and fostering other transnational illegal activities such as trafficking in arms, narcotics and humans. Growing evidence points in the direction of a nexus between terrorist groups and other forms of illicit activities, such as transnational organized crime, illicit trafficking of firearms, money laundering, and drug trafficking. While most of this cooperation appears to be motivated by tactical reasoning, strategic-level cooperation also occurs. For instance, drug trafficking represents a key source for the insurgency led by the Taliban in close interaction with AQ, influencing strategic and operational choices. Moreover, AQIM includes among its sources of financing a wide range of criminal activities, i.e. kidnapping, robbery, racketing and weapons smuggling.

Challenges and Opportunities

All these developments point in the same direction. First, it is unlikely that terrorism will become less of a threat in the coming years for the Alliance, thereby presenting a shared security concern for all Allies. Second, while counterterrorism measures traditionally rest with national authorities, i.e. law enforcement agencies and intelligence, the asymmetric nature of the terrorism threat and its root causes demand a comprehensive approach.

What is NATO's contribution to the fight against terrorism? And how must this role evolve in order to counter a changing threat?

It is important to understand how history shaped the Alliance's response to the fight against terrorism. The Alliance's previous Strategic Concept, agreed in 1999, had identified terrorism essentially as a risk affecting NATO's security but no practical measures were agreed by the Allies. This changed with the events of 11 September 2001, an event which shaped NATO's role in the fight against international terrorism in the early 21st century. Less than 24 hours after the attacks on the United States, NATO invoked Article 5, the collective defense clause of the Washington Treaty, for the first time in the history of the Alliance. The North Atlantic Council – NATO's principal political decision-making body – agreed that if it determined that the attack was directed from abroad against the United States, it would be regarded as an action covered by Article 5, which states that an armed attack against one or more of the Allies in Europe or North America shall be considered an attack against them all. Furthermore, eight practical measures were adopted by the North Atlantic

Council to support the United States.[11] Shortly thereafter, NATO launched its first ever counter-terror operation – *Operation Eagle Assist*. On request of the United States, from mid-October 2001 to mid-May 2002, seven NATO AWACS radar aircraft were sent to help patrol the skies over the United States. In October 2001, NATO launched its second counterterrorism operation - Operation Active Endeavour (OAE). OAE is a maritime surveillance operation in the Mediterranean which includes anti-terrorist patrols, escort and compliant boarding.

Following the momentum, NATO's 2002 Prague Summit demonstrated an increased commitment to counter terrorism, notably with the endorsement of the so-called "Prague Package." The Prague package aimed at adapting NATO to the challenge of international terrorism. The Alliance adopted a Military Concept for the Defense Against Terrorism (MC 472) that identified four pillars for NATO's military: first, anti-terrorism combines all defensive and preventive measures taken to reduce the vulnerability of forces, individuals and property to terrorism; second, offensive counterterrorism; third, consequence management, and fourth, military cooperation. Furthermore, the "Prague Package" included five nuclear, biological and chemical defense initiatives; protection of civilian populations; and a Civil Emergency Planning Action Plan as well as the NATO Response Force and the Prague Capabilities Commitment. In Prague, NATO also adopted the Partnership Action Plan against Terrorism that served as a framework document for counter-terrorism work with our Euro-Atlantic Partners. In 2009, the Action Plan was opened to the Mediterranean Dialogue and the Istanbul Cooperation Initiative partners on a case-by-case basis.

The 2004 Istanbul Summit reinforced NATO's determination by adopting further measures. At the Summit, NATO endorsed the creation of the Defense Against Terrorism (DAT) Programme of Work (POW) to improve the response to new security challenges posed by asymmetric threats. Regarding countermeasure technology development, the Defense Against Terrorism Programme of Work enhanced key measures to strengthen the Alliance's fight against terrorism where technology could help prevent or mitigate the effects of terrorist attacks. Due to the urgency of the challenge, most projects launched under the programme were focused on finding solutions that could be fielded in the near-term, for instance in the areas of countering improvised and force protection. Intelligence sharing was improved through the establishment of the Terrorist Threat Intelligence Unit, which became part of the new intelligence structure that was set up as a component of the

[11] The Allies agreed to enhance intelligence sharing and co-operation, both bilaterally and in appropriate NATO bodies, relating to the threats posed by terrorism and the actions to be taken against it; to provide, individually or collectively, as appropriate and according to their capabilities, assistance to Allies and other states which are or may be subject to increased terrorist threats as a result of their support for the campaign against terrorism; to take necessary measures to provide increased security for facilities of the United States and other Allies on their territory; to backfill selected Allied assets in NATO's area of responsibility that are required to directly support operations against terrorism; to provide blanket overflight clearances for the United States and other Allies' aircraft, in accordance with the necessary air traffic arrangements and national procedures, for military flights related to operations against terrorism; to provide access for the United States and other Allies to ports and airfields on the territory of NATO nations for operations against terrorism, including for refuelling, in accordance with national procedures; that the Alliance is ready to deploy elements of its Standing Naval Forces to the Eastern Mediterranean in order to provide a NATO presence and demonstrate resolve; and that the Alliance is similarly ready to deploy elements of its NATO Airborne Early Warning Force to support operations against terrorism.

ongoing intelligence reform efforts. In endorsing the Comprehensive Political Guidance at the Riga Summit in November 2006, NATO recognized that “terrorism, together with the spread of weapons of mass destruction, are likely to be the principal threats to the Alliance over the next 10 to 15 years.”

In sum, the most important strands of NATO’s work undertaken in the realm of counterterrorism up until the Strategic Concept 2010 were political consultations among Allies, the conduct of operations, the management of possible consequences of terrorist attacks, and the development of countermeasure technologies, intelligence and information exchange, as well as the provision of training and exercises for Allies. NATO also sought closer cooperation with partners and other international organizations to counter terrorism.

There are various important lessons learned from the past decade. First, due to differences among Allies in defining terrorism – as an enemy or as a crime – a coherent approach to ‘fight the menace’ has been difficult to agree upon. Regardless of the definition, however, the international community learned that terrorism can only be effectively countered through a mix of soft and hard power. This being said, the role of the military, while undeniable, is mainly, and should only be, supportive to political, diplomatic, legal, and (socio)-economic efforts. Second, the fragmented nature of the counterterrorism effort within NATO and the organizational culture pose a unique challenge for developing a coherent response to terrorism. For instance, Allies have not sufficiently engaged on exchanging views on broader security developments and threats such as terrorism or proliferation of WMD. Third and partly as a result of this underdeveloped consultation process, NATO has played mainly a reactive role in the fight against terrorism. Fourth, NATO has given too much attention to operations and military technology and had too little focus on what arguably is the key to effective counterterrorism, namely the preventive dimensions as well as coordination with other international efforts. Fifth, cooperation with partner nations and other international organizations has not been exploited to the full. For example, NATO has not taken local capacity building of partners sufficiently into account, although this has emerged as a vital component of prevention in the fight against terrorism.

Prospects of NATO’s Role in the Fight Against Terrorism After the Lisbon Summit

The new Strategic Concept reaffirmed NATO’s role as the unique and essential transatlantic forum for consultations and dialogue and set out collective defense, crisis management and cooperative security as core tasks of the Alliance. In the fight against terrorism, NATO can and must do more than it has been doing thus far. Needless to say, NATO’s overall role as an international organization in this effort is embedded in the broader effort of the international community led by the United Nations and supported by many other international, regional and sub-regional organizations. The task ahead is clear: If the Alliance wants to remain an effective security provider for its members contributing to the prevention of 21st century security threats, it must become more of a team player – outside its borders and within its borders. However, turning intentions into tangible policies will require a lot of hard work. NATO has only just begun to embark on this journey and different security priorities among Allies will not ease this journey. But the Alliance, a political-military organization, has more to offer than military power and capabilities alone. It has a legitimate role to play in the fight against terrorism by focusing on comprehensive measures in the civilian and military domains that include protection and prevention, not only emergency preparedness and consequence management.

First and foremost, as NATO is transforming from a defense alliance into a multi-faceted security organization, Allies need to change the way they think about terrorism and other emerging security challenges. For instance, the prevention of terrorism can only be achieved if Allies are sharing information with each other and consult with each other on terrorism and other emerging security challenges. This being said, I firmly believe that NATO's political horizon and consultations should not only be dependent on action and troops on the ground. Engaging in thematic discussions on international security would allow NATO to raise awareness about emerging threats, to apply lessons learned and to create an organizational culture that it needs in the security environment of the 21st century.

Second, NATO needs to broaden and deepen the number of initiatives to counter terrorism, taking into account cross-cutting threats stemming from cyber, energy, proliferation, instability and conflict in cooperation with Allies and its partners. To this end, NATO is reviewing its capabilities and countermeasure technologies in order to enhance its capacity to detect and defend against international terrorism. The aim is to alter NATO's ability to quickly and effectively respond to the evolving threat environment. Third, training, exercises and capacity-building are of great importance and the Alliance will need to use its assets more efficiently in order to leverage NATO's expertise and overall contribution to the fight against terrorism. In this realm, important assets of the wider NATO family are the Centres of Excellences. Centres of Excellences are international military organizations that work alongside Allied Command Transformation (ACT) in Norfolk, Virginia, in the United States. Although not part of the NATO command structure, they are part of a wider educational and training framework. Designed to complement the Alliance's current resources, Centres of Excellences cover a wide variety of areas, with each one focusing on a specific field of expertise what goes beyond what NATO HQ is able to provide. Engaging this network of centers more closely in NATO's work in the fight against terrorism will provide a tangible improvement to NATO capabilities. For instance, the Defense Against Terrorism (DAT) Centre of Excellence in Ankara, Turkey, provides subject matter expertise and training on how to best to counter terrorism, assists in the development of doctrine and helps to improve NATO's and partners' capabilities and interoperability.

Fourth, the Strategic Concept stresses the Alliance's preparedness to develop political dialogue and practical cooperation with relevant organizations across the globe that share NATO's interest in peaceful international cooperation. By recognizing the reality that coordination with other international actors is essential, NATO has taken a further necessary step to fulfill its key security tasks. Allies are required to seek new ways of connecting NATO with the broader international community by building structured relations in order to add value to the global effort undertaken in the fight against terrorism. In line with the comprehensive approach, NATO will improve its coordination with other international organizations through regular exchanges of views and information as well as by enhancing mutual knowledge of working processes to leverage the full potential of each stakeholder and to establish a pattern of cooperation and dialogue. In my personal view, the European Union is a unique and essential partner for NATO in the fight against terrorism, as both organizations share a majority of members and all members share common values. In order to realize a comprehensive approach to counterterrorism and deliver the best results for their citizens in times of diminishing resources, NATO and the EU must aim to deepen and broaden their cooperation in the field of information exchange, streamline capability development and external assistance to partners in all areas necessary. The United Nations is another key partner for NATO that offers much more in the fight against terrorism than merely a framework of legitimacy for the actions of the Alliance. NATO is and will actively support the UN Global Counterterrorism Strategy as well as other relevant UN Resolutions. Participation in regional and international efforts, for example at the Regional Expert Meetings on the Implementation of the UN Global Counter-Terrorism Strategy or the Special Meeting of the UN Counterterrorism Committee with international, regional and sub-regional foci, demonstrates NATO's firm commitment to the global fight against terrorism. Last but not least, the prevention of international terrorism can be best achieved through engaging with a wide range of partners. NATO has today more than 30 partner countries that participate in more than 1,500 activities annually. Depending on individual programmes, NATO will strengthen its partnerships in the fight against terrorism. The Alliance will seek to enhance consultations, information sharing, leverage lessons learned and provide tailor-made training, exercises and courses that support national, regional and international efforts in countering terrorism. Through tools such as the Science for Peace and Security Programme, NATO will further reach out to civilian actors in partner countries to promote projects and events in areas such as human-behavioral science, cyber terrorism, the protection of critical infrastructure and the detection and defense against CBRN terrorism.

Conclusion

The dynamic and evolving nature of the international terrorism threat requires that the Alliance's response is comprehensive and flexible. Implementing the levels of ambition embodied in the Strategic Concept, NATO will seek innovative ways to demonstrate the added value it can provide to the protection of the Alliances' populations against these challenges. The establishment of the Emerging Security Challenges Division in the International Staff at NATO is a good start. In responding to these 21st century challenges, a new approach of ***protection, prevention and partnering*** will allow NATO to continuously adapt to the complex and diffuse threat environment while effectively countering terrorism and addressing its root causes. Coordination with all strands and stakeholders within the Alliance as well as with partners, other international organizations and networks involved will be key to realize the Alliance's mission. NATO will ensure that the Alliance remains an unparalleled community of freedom, peace, and security and shared values and continues to be effective in a changing world, against new threats, with new capabilities and new partners.

Defence Against Terrorism Review
Vol.3,No.2,Fall 2010,pp.13-22
Copyright © COE-DAT
ISSN: 1307-9190

Cyberattacks Against Estonia Raised Awareness of Cyberthreats

Jaak AAVIKSOO
Minister of Education and Research, Estonia

Abstract: *NATO has just agreed on its first Strategic Concept since 1999. Cyberdefense and cybersecurity occupy a prominent position in NATO and her allies' strategic thinking, but they represent so much more than a new security problem. Growing cybersecurity problems are a fact of our irreversible and irresistible movement toward an ever more interconnected and information-based world.*

Keywords: *Cyberattack, Estonia, Cyberdefence, Cybersecurity, Cyberterrorism*

Introduction

In April 2007, Estonia experienced a coordinated and massive attack against government infrastructure, financial service providers and domestic media. These attacks, intended to destabilize the government and foment civil unrest, were conducted entirely in cyberspace. While not the first cyberattacks, they represented the most sophisticated and clearly politically motivated attacks to date, and have come to be known as a "digital Pearl Harbor." After the attacks, Estonia made a conscious choice to publicize the extent and nature of the attacks, start a policy discussion on the centrality of cyberdefense to security, and push our Allies in the direction of concerted action, doctrinal change, and cooperation. Since then, Estonia has been at the forefront of international debate on cybersecurity and cyberdefense.

Estonia feels the sting of cyberthreats particularly sharply. We are a highly connected and web dependent society; 98% of bank transactions go over the web and people use the Internet to pay taxes, access medical records, and even vote. We are also a small country with limited natural resources. Our economy is dependent on trade and connections with the outside world. Our experiences embody the strategic bind of all developed countries: interconnectedness, openness, and technological dependence constitute our strengths, but they also form an Achilles heel. Those who would challenge our societies, our values, our economic power or our military strength know to focus their efforts on this major chink in our armor. In my brief presentation, I will focus on how Estonia's strategic thinking has reacted to cyberthreats and how we must cooperate to secure cyberspace as a whole

In no small part as a result of these attacks, the last few years have been a period of growing awareness of the problem and new attention to concepts like cybersecurity, cyberdefense, cyberdeterrence, cyberterrorism and cyberweapons. The defense community is now moving from an awareness-building stage into an institution-building and doctrine implementation phase.

Why Cyber Matters

In the last three years, we have spoken much about how 'cyber' presents a fundamental paradigm shift in the global security dynamic. Cyberthreats epitomize asymmetry: they are inexpensive and easily developed, they neutralize the conventional military superiority and secure position of Western countries, and leave the world's most technologically advanced and networked societies most vulnerable.

Cyberattacks are cheap to launch, requiring only the cost of minimal hardware and manpower. The tools of cyberattack are widely available to both states and non-state actors, from organized crime to the disgruntled lone hacker. The source of a cyberattack can be difficult to determine, as a cyberattack can be routed through third parties and countries, co-opting networks unrelated to the attacker or target. In cyberspace, there are no clear distinctions between combatants and non-combatants. Civilian targets are both valuable and easy to attack.

Our societies' vulnerability extends beyond a mere threat to critical infrastructure. Information societies depend on trust and open communication. Undermine these, and you can spread panic, destabilize democratic governments, and destroy massive amounts of wealth. Cybersecurity and defense is often spoken of alongside other so-called 'new threats' like energy security, climate change, or population movements, but cyber is more than a security and defense problem, a change in the structure of our societies, economies, and relations. Instead of talking about cybersecurity and cyberdefense, we need to speak of security and defense as a whole in a cyberworld.

Demystifying Cyber: Similarities to Existing Security Challenges

These risks from cyberspace have led to a certain aura around questions of cyber-security and cyberdefense. I would like to demystify these terms and consider how we can and must adapt our existing institutions and solutions to function in a cyber-and-information world. We do not have the luxury of reinventing the wheel, nor do we need to.

Cyberattacks and dangers share fundamental similarities to more conventional threats. Ultimately, real people launch and order cyberattacks, using hard physical infrastructure such as servers, power lines, and data connections located in real places. Cyberattacks are guided by calculations of self-interest and risk, either individual or collective. There is a gradient of threats and capabilities, from hackers to states.

My talk is broken down into two parts: in the first section, I will look at the risks to modern society as a whole that arise from cyberspace. I will recommend we adapt a comprehensive approach to cybersecurity that integrates domestic security thinking in every country and creates meaningful international cooperation. In the second section, I consider the narrower implications cyberattacks have for militaries, ministries of defense, and our defensive alliances. Over the course of 45 minutes, I hope to outline strategies for making our societies as a whole, our existing defenses, and our international cooperation more resilient to cyberattack and able to navigate the straits of 21st century security.

A Comprehensive Approach to Security, Making Us More Resilient

The Old Model: Defense and Security are External and Internal Threats

We tend to distinguish between security and defense problems. Our common sense tells us security problems relate to internal threats, while defense threats come from outside. Historically, this division has made particular sense for the United States, for whom two oceans have helped separate external threats from domestic security concerns. This division does not work in cyberspace.

Asymmetric Threats Like Cyber Require a Comprehensive Approach

Cyberthreats disregard borders. Oceans do not provide a natural barrier against ones and zeros. Any cyberdefense will inevitably entail mitigating the effect of potential attacks. Securing cyberspace is thus largely a question of societal resilience, and requires you to ask: are your institutions, agencies, private sector, individual users able to absorb and bounce back from shocks and attacks?

Cooperation and a Multisector Approach

Following our 2007 cyberattacks, we came to several key conclusions. We realized that the old dividing lines between domestic and international conflicts, defense and security problems, law enforcement and military solutions, public and private do not hold in cyberspace. No single ministry or department can handle what is simultaneously a problem of infrastructure, defense, law enforcement, commerce, and civil liberties. Furthermore, 85% of web infrastructure is in private hands. Therefore, 80% of cyber-attacks are launched against private companies, NGOs, and individuals.

These challenges mandated a multisector approach and cooperation with the private sector. We developed a National Cybersecurity Strategy, which we adopted in 2008. The strategy offers a common vision for all actors in society on how to reduce our vulnerability in cyberspace. The document envisages specific guidelines for government and the private sector, universities, NGOs and citizens. Our goal is to resolve decision-making ambiguities that arise during fast-paced cyberconflicts, divide responsibility so as to make optimal use of our limited resources, ensure that our entire webspace is secure by including the private sector in developing a high level of security standards, and instill a general cybersecurity culture.

The notion of good cybercitizenship is crucial. We believe that a precondition for securing cyberspace is that every owner of a computer, computer network or information system feels responsible for the expedient and prudent use of information and communications technology. We achieve such good cyberhygiene through both regulation and awareness campaigns. Simple steps like updating virus software and downloading files responsibly slashes the risk of identity theft, data loss, quickly-spreading viruses, and botnets. Consider if computer users in the US and Canada had employed better cyberhygiene, many of the attacks against Estonia in 2007 simply would not have occurred.

We have included cyberscenarios in our crisis planning and have conducted comprehensive exercises and tests of our systems that include all sectors of society. In order to constantly learn and adapt, we strive toward a culture of informal cooperation, openness to criticism and learning from previous errors.

We have also found an innovative solution to the difficulties of finding qualified manpower to tackle cyberdefense. We have created a 'cyber' division in our all-volunteer home guard. Should we be subject to another cybercrisis, we will have a large pool of IT specialists, programmers, and hackers to help carry out an effective defense.

Admittedly, Estonia's small size gives us flexibility. We can literally gather key players from all sectors of society into one room. The combination of our small size and early adopter approach to information technology make Estonia the perfect test-bed for experimenting with new approaches to cyberdefense and security. This is one of the potential areas of deepened US-Estonian cooperation I have discussed with my counterparts during this trip.

International Cooperation

Cyberspace is global and no country is a 'cyberisland.' Cybersecurity today is in the same phase of development as maritime security in the 18th century. Cyberattackers honor no flag or national border. The state still has a long way to go before achieving a monopoly on the use of force. If the ability to instantly cross borders gives cybercriminals and cyberattackers a measure of impunity, we have but one choice: to extend the long arm of law and order across borders.

There is growing international cooperation between experts and policymakers, and international best practices are starting to evolve. While informal cooperation is good, the current level of contact occurs on too *ad hoc* a level. This cooperation needs to be formalized.

Existing EU and NATO structures are a good place to start formalizing such relationships. Both need to adapt their chains of command and decision-making procedures to the contingencies of fast-paced cyberconflicts. NATO is the best place to address many high-end cyberthreats, but it cannot solve all problems. The EU, with its experience in institutionalizing civilian cooperation, is a natural player and partner for the US. Sadly, NATO and EU coordination problems only amplify existing coordination difficulties among civilian and military structures that work in parallel with little communication.

To combat both criminal and state-sponsored threats, we need better detection and analysis of attacks. The same sensor networks, libraries of malicious code, collaboration among cybersecurity crisis management centers, and agreements with ISPs to allow access to potentially sensitive data in times of crisis that we need to deal with cybercrime will also allow us to defend ourselves against malicious politically-motivated cyberattacks. Civil-military cooperation is, as elsewhere, essential here.

The US has urged NATO to build a cybershield that would consist of a comprehensive network of sensors, response teams and analysts to identify and quarantine incoming cyberattacks against military and civilian targets. The more nodes such a network has and the greater its reach, the more it benefits all involved. This is a fundamentally sound idea that needs more fleshing out. Developing such defenses is one of Estonia's and NATO's priorities following the new strategic concept, one we hope to work very closely with the US on.

Ultimately, this cooperation cannot be limited just to EU or NATO countries, nor can we neatly divide up responsibility between different international organizations. For instance, all democratic countries have a joint interest in IT forensics capabilities that do not tread on civil liberties. Rather, our needs call for a real spirit of trust and cooperation.

On the level of cybercrime and 'hacktivism,' a legal solution is possible. Rooting out cybercrime and cyberattacks carried out by non-state actors is a good step toward securing cyberspace as a whole. Although cybercrime only makes up part of the range of threats from cyberspace, it is a domain of lawlessness that constitutes a threat to all states and to the global commons; limiting cybercrime is in everyone's interest. Countries outside of Europe should sign on to the Council of Europe's Convention on Cyber Crime. In addition to mandating cooperation, the convention also sets a standard for domestic legislation. The willingness of third countries to be a party to this treaty is good proof of whether the goodwill to tackle international cybercrime is there. International law is in this case a boon to everyone's sovereignty.

Law enforcement has its limits. We cannot always identify perpetrators. Pariah states offer safe haven to cybercrime and terrorism. Certainly, no amount of international law has thus far ended war as we know it. States will be willing to channel their considerable resources into using cyberweapons towards political and warlike ends. Thus, we also need solutions for dealing with cyberwar.

Thinking of Cyber Defense in a Conventional Defense Context

Example: A Crippling Attack Against the EU or US

Consider the following potential cyberattack: one day, the US or EU wakes up to find electrical power stations shut down; communication by phone and Internet disabled; air, rail and road transport impossible; stock exchanges and day-to-day bank transactions frozen; crucial data in government and financial institutions scrambled and military units at home and abroad cut off from central command or sent fake orders. The attack is particularly effective because it combines sophisticated cybertechniques with traditional spies who can bypass safeguards designed to isolate secure and critical networks and physically connect these to the internet. A recent report put the cost of orchestrating precisely such an attack at about 150 million lira and 750 people working for one to two years. This represents a fraction of the cost of carrying out such an attack using bombs and traditional sabotage, but still requires complex coordination and a long-term investment in manpower and resources. Such attacks remain the preserve of states and state-sponsored groups.

We Still Need Military Defense Thinking for Cyber-Conflicts

The importance of strong cybersecurity in ensuring national security and mitigating the effects of all levels of cyberattack has led many to use the phrase 'cyberdefense' and 'cybersecurity' interchangeably. We are seeing, however, that the state has not fully lost its advantages and superior power in cyberspace. Allow me, thus, to contradict myself: when we are dealing with a state-launched or state-sponsored attack, or when an attack threatens critical infrastructure or the stability of a society, we must adopt an explicitly defense-oriented paradigm.

Many Countries are Developing Terrifying Cyberweapons

The militarization of cyberspace is currently under way. A number of countries have acknowledged that they are developing 'cyberweapons' for offensive use. At this level of development, there is a strong offensive advantage that even the best cybersecurity cannot mitigate. Cyberattacks can be combined with the conventional and intelligence capabilities available to states, magnifying their impact. While not as terrifying as all-out nuclear war, cyberattacks can damage physical infrastructure, cause loss of life, and sow widespread fear and panic that can quickly destabilize networked societies. In short, full-scale cyberwar could bring modern life to a halt.

Arms Control and Deterrence are an Uphill Battle in Cyberspace

Unfortunately, the standard logic of arms control is greatly complicated in the case of cyberweapons. There is no single weapon to control. The damage from cyberattacks comes not from technology, but its coordinated and targeted use. Consider loading a government website on your browser – a completely legal, innocuous activity. Yet when networks of thousands of computers are directed to simultaneously and repeatedly access the same networks for hours on end, it becomes a coordinated cyberattack. Even in the case of clearly mischievous acts, like breaking into a website or inserting malicious code, the difference between a lone hacker testing his skills and a state-sponsored attack is one of degree and organization, not of kind. Furthermore, challengers to our security have every incentive to develop and field cyberweapons and little reason to abide by a 'cyberarms' control regimen.

We can never fully solve the attribution problem in cyberspace. Whereas the source of an incoming missile is easy to discern, cyberattackers can mask their tracks. Misattribution can raise tensions and escalate conflicts. The attribution problem is compounded by cyber militias and hacktivists who may receive training, direction and technical assistance from states, but do not follow orders or even reside in the state. Such hacktivists have played a role in nearly every major cyberconflict. For these reasons, credible arms control and deterrent regimens would currently be challenging to establish.

Developing a sensor network will help address these problems; so will good human intelligence. Even when attribution is impossible, we can still rely on an obligation to assist. Governments have an obligation to assist if an attack is routed through their country or perpetrated by an attacker located within their country. A failure to do so amounts to complicity in the attack, potentially in a manner similar to the Taliban's complicity in harboring Al Qaeda in Afghanistan.

Given man's history of conflict, we should not rely too strongly on the hope that destructive cyberconflicts will not occur. This sad fact reinforces the need for strong cybersecurity measures to increase our resilience against cyberattacks. Such defenses also serve as a form of deterrence by denial, preventing potential aggressors from benefitting from cyberattacks. As the likelihood of malicious cyberattacks by a state or state-sponsored group does go up, we must give thought to how our collective defense and alliances will react.

How Do Collective Security Guarantees Apply to Cyberdefense?

There has been a great deal of hand-wringing over how collective security guarantees, particularly the North Atlantic Treaty and the EU's Lisbon Treaty, apply to asymmetric threats like terrorism or cyberattacks. Does collective defense apply when lines of code take the place of bombs and bullets? I would argue this is the wrong question to ask.

The decision to invoke NATO's Article V (or the EU's Solidarity Clause) should not depend on the type of weapon used or the identity of the attacker. Article V comes into force in the case of an armed attack (the EU Solidarity Clause is even broader). Neither specifies what constitutes an armed attack, nor should they: technology and military practice changed in leaps and bounds during the 20th century, and there is no reason to believe the 21st century will be any different.

Our primary criterion must be the type of damage caused. Did an attack cause a loss of life, large-scale economic destruction, or damage to infrastructure? Did it intend to? To account for cyberattacks, we need merely to maintain 'cyberequivalency' because an attack in cyberspace warrants a response equivalent to what we would do if the attack had used kinetic means.

NATO's Article 5 Innovation After 9/11 as an Example

NATO's reaction to the attacks of September 11 illustrates these points. Civilian aircraft were turned into dangerous weapons as a result of the intentions of the attackers and the choice of their targets. NATO declared that an attack that resulted in the loss of thousands of lives and massive material damage was grounds for invoking Article V, regardless of the means used. Furthermore, the North Atlantic Council invoked Article V on September 12, 2001, only a day after the attacks had occurred, and as the identity of the attackers was still being sorted out. What mattered was the fact of the attack, not the identity of the attackers.

Collective Security Works Because it is Flexible

The very strength of Collective Security guarantees lies in their flexibility, which allows them to adapt to changing circumstances while maintaining the promise of collective security. NATO in particular has adapted to a changing world for 60 years, and will continue to do so. We should not artificially tie our hands or restrict that strength.

Military Preparation

Issues in cyberspace will not simply supplant existing problems. We must see cyberspace as an additional military dynamic that will contribute to an already crowded 21st century battle space. US Deputy Secretary of Defense William Lynn put it best when he called cyberspace a new domain of operations alongside land, air, sea and space.

In addition to threatening civilian networks, cyberattacks can target military systems directly, taking weapons and communications systems off line. In sum, as the US Air Force Cyber Command's strategic vision states, controlling cyberspace gives you "the potential to achieve victory before a kinetic shot is fired."

We must therefore harden our militaries against cyberattacks. If our conventional military advantages are reduced to naught, we face a deep crisis of confidence in our security architecture. NATO and individual allies should see cybercapacities as a major priority in force renewal.

The battlefield of the future will be a mixed one, where cyberattacks complement kinetic attacks. Georgia's experiences in 2008, where sophisticated cyberattacks and a well-organized propaganda effort supplemented a conventional offensive, suggest that there is no clear division between asymmetric and symmetric, conventional threats. 'Cyber' is the inescapable future of all militaries, and of NATO.

Cyberdefense is an area where NATO as a whole is on board. Despite cutting billions from their defense budget, the UK's recent Strategic Defense and Security Review allocated GBP 650 M and attention to cyberdefense and cybersecurity. Numerous other European allies have gone through review processes and similarly concluded to devote far greater attention to cyberspace. This past weekend, both Angela Merkel and British foreign secretary William Hague delivered major addresses on cyber defense.

Cyber-Consciousness in NATO's SOP

To counter these risks, NATO as an organization needs to work cyber into its daily thought. Military exercises should take into account cyber risks, and conduct stress tests of critical infrastructure. NATO needs practical exercises that cover detecting and analyzing cyber attacks, reacting to potential cyber-Article 5 situations, and decision procedures in the case of such an attack. Such exercises will reveal current weaknesses and unresolved doctrinal questions. NATO also needs to ensure robustness in its lines of communication to each member state, in its command and control systems, and in its logistical abilities. I am hopeful we can translate the positive momentum from adopting our Strategic Concept into realizing these changes.

NATO is debating how much responsibility the Alliance should carry for protecting key civilian critical infrastructure. NATO cannot alone protect key civilian infrastructure. NATO should, however, take a lead role in creating uniform standards and policies. The

Our defense establishments also need a culture of welcoming dissent and well-intentioned criticism within the defense sector. Junior officers or government officials who raise concerns about cybervulnerabilities should not see those concerns and their careers sidelined. Rather, they need to be empowered to participate in solving these problems, and be given constructive forums for voicing concerns within the chain of command. A top-down institutional culture will not allow us the flexibility and adaptability we need.

NATO CCDCOE in Tallinn

Estonia has played a strong role in developing cyber thinking and readiness in NATO. The NATO Collaborative Cyber Defence Center of Excellence, located in Tallinn, is investigating the legal, policy, civil defense, strategic and tactical ramifications of the issues I have been covering**.** We are bridging the gap between current thinking and the strategic and doctrinal clarity threats from cyberspace require.

Conclusion

Cyberthreats constitute a profound revolution in the nature of threats to peace and the functioning of 21st century economies, states, and societies. In dealing with these changes, we have drawn three conclusions:

- First, the challenge from cyberspace is not primarily a technical challenge, but a question of leadership. Will we properly leverage our capabilities, resources, and brains? Are we willing to challenge our preconceptions, study our weak spots, and test our systems in taxing exercises?
- Second, achieving cybersecurity requires a combined, multisector, comprehensive approach that focuses on building civil-military relations, cooperation with private enterprise, and educates the citizen.
- Finally, cybersecurity and defense require an increased level of formal and informal international cooperation. Where possible, we should adapt existing structures and agreements, including the Council of Europe's convention on cybercrime. When necessary, we should design new approaches.

At every step, we should rely on the strength of the NATO, the trust we share as allies, the values we hold dear.

Defence Against Terrorism Review
Vol.3, No. 2, Fall 2010, pp. 23-36
Copyright © COE-DAT
ISSN: 1307-9190

From Hit and Run to Invade and Stay: How Cyberterrorists Could Be Living Inside Your Systems

Alan E. BRILL
Senior Managing Director, Secure Information Services, Kroll, Inc., Washington DC, United States

Abstract: *In recent years, there has been a distinct – and troubling – change in the tactics used by cybercriminals (criminals who have the technical skills to exploit weaknesses in digital technologies)and the cyber-elements (the terrorist organization members or those willing to work for them – for money or reasons or belief – who have the skills to exploit those same weaknesses) of terrorist organizations. They have gone from a hit-and-run mentality to one that stresses gaining and maintaining long-term access to the digital infrastructure of their enemies. These new tactics have worked, and worked well. But the tools of these cyber-invasions can be used in many ways. The same techniques that can gather intelligence can be used to prepare to disrupt or disable technology-based targets, ranging from factories to military communication systems. In this paper, we try to describe the evolution of the threat, and suggest ways to meet the challenges posed by the Advanced Persistent Threat scenario.*

Keywords: *Cyberterrorism, Cyberdefense, Hacking, Networks, Security*

Introduction

The ever expanding use of computer systems to process information – including sensitive tactical, strategic and financial information – not only by governments, but by corporations and individuals as well, has created incredible targets for cyber-skilled terrorists and criminals to exploit in order to fund their activities and to collect information to assist them in carrying out their plans.

One of the characteristics of this expansion has been the adoption of these technologies by significantly more small- and medium-sized governments and corporations. For example, the ability to initiate and approve wire transfers online has created an opportunity to steal literally millions of dollars in minutes.

But to best exploit these opportunities, there has also been an evolution in some basic concepts that information security people took for granted for many years. It was assumed that those stealing sensitive information or money were going to get into the target system, exploit it and get out as quickly as possible. While there are unquestionably incidents where the hit-and-run mentality applies, the ability to get into a system, hide there and gain intelligence, cause problems, exfiltrate data and hide evidence of the wrongdoing is now the more common approach.

What this means is that where cyberdefense has been traditionally focused on the enemy who is outside and trying to get into the system, the new reality is that with the use of zero-day techniques (exploiting security weaknesses in ways that have never been used before) and the delays in making defenses to newly-discovered problems widely available (through anti-malware updates) it is necessary to assume that the enemy is already inside of your system. You have to be able to recognize and defeat the attacker from within your environment as well as the attacker outside your system perimeter.

In addition, the expansion of the use of automated banking and sensitive information processing by small and medium organizations means that the number of targets available to the cyberterrorist or cybercriminal has grown. And those new targets may not have the experience, the staff or the budget to protect themselves as thoroughly as larger organizations or governments can.

If the evolution of the threat is not realized, the advantage can turn to the attacker,but through understanding and proper planning, that advantage can be countered.

The Worst Case Scenario: The Enemy Inside Your Systems

If you are considering the security of a computer network used to process highly confidential and proprietary information, what is the worst case scenario?

- *Destruction of the network?* Most networks have plans in place for disaster recovery and continuity of operations.
- *Denial of service to users?* True, so-called distributed denial of service attacks can use thousands of computers to send enormous volumes of requests to a system to overwhelm it and knock it out of production, but there are effective safeguards available to rapidly detect and defeat most attacks of this kind.
- *Network Intrusion?* Yes, this is bad, but it is usually recognized, and you can investigate the cause and strengthen your defenses.

I would like to suggest that the worst case scenario is an enemy who gains surreptitious access to your systems, who can stay below the radar of your defenses, and who can have access to your systems and your information for periods of months or years without being detected. A long-term intruder who can get in and stay in – and who you do not even know is there – is a nightmare scenario. But this nightmare is all too real. Consider the following:

> In 2008, the U.S. Department of Defense suffered a significant compromise of its classified military computer networks. It began when an infected flash drive was inserted into a U.S. military laptop at a base in the Middle East. The flash drive's

> malicious computer code, placed there by a foreign intelligence agency, uploaded itself onto a network run by the U.S. Central Command. That code spread undetected on both classified and unclassified systems, establishing what amounted to a digital beachhead, from which data could be transferred to servers under foreign control. It was a network administrator's worst fear: a rogue program operating silently, poised to deliver operational plans into the hands of an unknown adversary.[1]

The intrusion that U.S. Deputy Secretary of Defense Lynn is describing in that quotation went undetected for an extended period. In spite of extensive security measures, it spread through classified and unclassified networks;its operation over time was not caught. It was, perhaps, the ultimate infiltrator, providing valuable intelligence from an enemy who did not even know that it had been successfully attacked.

Looking at cases of intrusion across the public and private spheres, information security experts have seen an evolution in the thinking or adversaries. Where they were formerly content to follow a hit-and-run-and-hide strategy, their motive is now to get in, hide, and stay in target networks, prepared to exfiltrate data, or cause destruction at a time and of a kind (including the placement of false information, reduction or elimination of digital communication to forward deployed forces, etc.) chosen by the attacker. This is not to say that we have seen a complete shift to the new motive – far from it. Hit and run attacks to steal information, money or things of value (like credit card numbers) are still very popular. But anyone who ignores the new reality in which attacks can be very stealthy and very persistent is likely to find that the enemy is not just at the gates, but is already deep in their systems, watching, reading, and preparing for future actions.

Cyberattack Strategic Evolution

As data moved onto Internet-connected computers in almost unimaginable volumes in both the public and private sectors over the past two decades, hackers, criminals and terrorists kept pace. They understood the potentials for misusing the technology. As Scott Charney, formerly the head of the U.S. Justice Department's cybercrime section, now the Corporate Vice President for Trustworthy Computing of Microsoft, said in a television interview about hackers, "[a]t any given moment, there's a percentage of the population that's up to no good"[2] and he was right. Hacking and computer intrusions became issues that both governments and corporations had to worry about. Computer security became something indisponsible for governments and corporations moving into the new world of computers, and ultimately into the even newer world of the global Internet.

Starting out as just a technical issue of concern to information technology specialists, computer security has become something virtually everyone thinks about. From identity theft to the compromise of hundreds of thousands of credit card numbers, it has entered the global consciousness.

Over the years, as the technologies involved in computer networks and the Internet have evolved, so have the threats.

[1] William H. Lynn III, "Defending a New Domain,"*Foreign Affairs*, Vol. 89, No. 5, p. 97.

[2] Scott Charney, "Highway Robbery," *CBS 60 Minutes,* DATE.

Early threats were usually hit-and-run. Someone broke in, stole something – perhaps a blueprint or a set of documents – and left, attempting to leave behind as little evidence as possible. Perpetrators became skilled at manipulating internal system log files to cover their tracks.

But as networks evolved, new threats emerged, and some of them turned out to have the desirable characteristic (from the view of the attacker) of being able to be used over and over, either against multiple targets, or even against the same target. For example, as Internet-interfacing systems gained connectivity to traditional large-scale computer databases, the intruders discovered that many systems had a flaw that allowed them to manipulate the form of request that their computer sent to the Internet server of the target machine. It could contain instructions directed not to the web server, but to the back-end database. If the website's security was not all that it should be, the web server would pass the request along to the database, which could process the request and respond with data that it normally would not provide to an external user.

For example, in a recent case, a U.S.-based financial services firm was told that customer financial information was being misused for identity theft, and the pattern of victims showed that the data had to originate from their company. Our investigation showed that they had a number of customers on an old computer system that had been scheduled for replacement two years earlier. However, due to budgetary restrictions, the replacement of the system had been postponed multiple times. The old system still worked, but it only received attention from the programmers when there was a specific problem. It was a very low priority system from the company's viewpoint. But because it was obsolete and had not been updated in years – including its security – it was certainly a high-priority target for an attacker. The attacker targeted this system and used the technique described above – called a "SQL Injection Attack" to send questions to the database engine behind the website.

When you enter an address into a web browser – for example "www.google.com," you think of it as an address, but it can contain more. For example, if you go to the Google search engine and enter "cyberterrorism" as your inquiry, that is transmitted to Google as a web address that specifies the inquiry (along with other parameters). Google's servers can interpret this as a search request and process it appropriately. But in a SQL injection attack, the attacker is seeking access to data that is not intended to be released. By crafting inquiries that contain elements of Structured Query Language (SQL), a standard way of expressing data base inquiries, an intruder tries to send commands directly to the database, bypassing the web server and its security features. If the system is not designed with controls to prevent SQL commands from being executed, an intruder can start sending commands to see what information can be extracted.

By looking at the response to test questions, the intruder was able to figure out what data was available, and how to get to it efficiently. Over a period of days, the intruder sent tens of thousands of inquiries, all written with the SQL code embedded, and the system ultimately responded with the detailed and highly confidential data of more than 30,000 customers.

All of this was recorded on log files, but because this old system was regarded as being low-priority, the logs were never looked at by anyone.

Once we understood the attack vector (how the intruder was getting in – repeatedly – to the system and extracting data) we had to tell the victim company that the system could have been adequately detected against this kind of attack by the use of a free, open source web application firewall program. The process of downloading, installing and tuning this program for optimum performance and putting it into live operation took one of our engineers working with the client less than 90 minutes to accomplish. While the attacks continued, they were no longer successful, and the ability to recognize the attacks in real-time was an important tool for tracking down the perpetrator.

In this case, the company never knew that there was a problem until confronted with it from an external source. Literally millions of dollars of damages could have been avoided had anyone taken the time to look at the software and assess its vulnerability.

What is vital to keep in mind is that this was not a one-time attack. The attacker was able to use the same attack against the same target over and over. The attack had the characteristic of persistence. The attacker wanted to be able to visit whenever he (or she) chose to in order to harvest more information. Granted, the actual method of attack – the SQL injection – was not very stealthy. In fact, everything that happened was logged, which enabled the investigative team to know with great certainty which records had been compromised and which had not. And it was not very sophisticated as these attacks go,but it had the advantage of working, and yielding tremendous returns for the time invested by the attacker.

Over time, the means of attacking networks in a way that permitted persistence of intrusion, have gained in sophistication and subtlety. These means became associated with attacks that appeared to be committed by nation-states, including hits against high-value targets (as in the attack described by Secretary Lynn in Foreign Affairs Magazine) and even was reported during the last U.S. presidential elections. According to well-known author Bob Woodward, both the 2008 Obama and McCain presidential campaigns had been hacked by very sophisticated hackers – perhaps even by nation-states. The attacks were detected and both campaigns were notified. They took steps to defend themselves in ways that they had not previously employed. According to Woodward, when then-candidate Obama recognized that the intruders could have done more than steal data – they could have destroyed data as well – he said "this is important."[3]

While Admiral McConnell, then serving as Director of National Intelligence was focusing his briefing on acts committed by nation-states, the same technical tools are available to terrorists and to those out for personal gain. Someone once pointed out that if you are shot through the heart, the age, sex, weight and motive of your attacker is irrelevant to you. Regardless of the answers to those questions, you are dead.

Admiral McConnell said that the U.S. intelligence community found the intrusion into the computers being used by the Obama and McCain campaigns because the intruders were "clumsy." Can we base our defensive strategy on the hope that the bad guys will always be clumsy or inept? What if they are not? What if they are really good at what they do?

Let us look at the latest evolution of the ongoing contest between cyberattackers and cyberdefenders. It's called the Advanced Persistent Threat – or "APT." While different writers disagree on how to define it (and even how advanced it is), it is a real problem, and one that those who manage national issues of defense against terrorism have to understand.

The objective here is not to make anyone a computer technician, but rather to provide an

[3] Bob Woodward, *Obama's Wars*, Simon & Schuster, New York, New York, USA, pp. 9-10.

understanding of the motives, methods and problems associated with the latest evolution of the threat that we are facing, which may have enabled an attacker to read your emails, copy your documents and prepare your networks for disruption, even as you read this journal.

The APT Strategy

There is no globally agreed-upon definition of an Advanced Persistent Threat attack. In fact, writing in IT World's online publication, Kevin Fogarty has pointed out that "Advanced Persistent Threat has become the hot buzzword for an irresistible digital attack that should result in no blame whatsoever to the security, IT and business people involved – who, in fact, should get a raise and some time off for having endured such a harrowing experience."[4]

Fogarty is right. There is a tendency to use the term far too broadly. Traditional malware attacks are not by definition APTs. In fact, APTs can probably be better understood by members of the intelligence community than the technology community, since they use the traditional concepts of intelligence operations, aided, of course, by the latest in Internet and hacking technologies.

While APTs are closely associated with computer hacking, the perpetrators of APTs are willing and able to use the full range of intelligence resources,

They can conduct surveillance, both through online research and good old-fashioned feet-on-the-ground methods.

They use what the computer security community called "social engineering" – getting people to tell them things they should not. You might think that the fancy thumb drive you received is a gift from a vendor (after all, it has the vendor's name on it, and the accompanying letter certainly seems to be on their letterhead) but is it really from them, or is it a way to get you to introduce malware into the network? For example, in a number of recent incidents of fraudulent wire transfers involving the theft of millions of dollars, it was determined that the attackers used a two-stage strategy. In the first phase, they researched their targets to determine the names of financial executives and the bank the company used. They then called the bank and used what hackers call "social engineering," which is nothing more than getting an employee to reveal information that they should not divulge. They talked the bank's customer service people into giving them the credentials to enable them to access the online wire transfer system.

Once they had the credentials, they were able to access the bank's systems, get reports showing the numbers and balances of accounts, and when the moment was right, when the right amount of money was in the accounts, they initiated wire transfers, and millions of dollars moved around the world. According to logs maintained by the bank, the total time required to log into the system with the identity of an authorized financial officer, initiate the wire transfers, log in as a second authorized person, confirm the wires, and for the wires to be processed and completed was less than two minutes. In that two minutes, almost two million dollars was stolen.

[4] Kevin Fogarty, "Advanced Persistent Threat is the Best Fake Excuse for Data Breaches" *IT World* (online) April 19, 2011, at http://www.itworld.com/security/157361/advanced-persistent-threat-best-fake-excuse-data-breaches (accessed April 27, 2011).

From the viewpoint of terrorists, using techniques like this one represents a way of getting tremendous amounts of funds quickly and efficiently, with little risk. By quickly transferring funds around the world, the trail that investigators must follow quickly grows cold.

Add to this that the cyberterrorist or cybercriminal can initiate all of this from anywhere in the world, and to the investigator, the attack seems to come from any of a million or more computers belonging to innocent people whose machines have been turned into 'zombies' by malware (malicious software) that enables them to be remotely controlled.

Cyberterrorists can put undercover agents in place, perhaps as employees, perhaps as vendors. For example, janitorial staff is in offices late at night, has a great deal of access, and is often minimally supervised. Not a bad disguise for an attacker to use to be in a position to put a USB memory device into a computer unwisely left running and unprotected to upload a virus into the network. Or they may walk in the front door as a temporary worker. We have seen cases where completely unvetted 'temps' (temporary worker) have been given access to highly sensitive information, particularly if it is discovered that the temp has a high degree of skill with complex graphics or spreadsheet programs.

Just because traditional hacking focuses on stealing data of value to the thief – like credit cards or antiterrorism plans – do not assume that trait fully defines what an APT is directed against; for example, a military, intelligence or political organization would have other data as the objective.

A summary of an article in the U.S. Air Force's Strategic Studies Quarterly[5] describes a possible scenario for a cyberwar in 2020. The nature of the war did not involve conventional acts, but involved disrupting military networks and injecting false information into the networks.[6]

In an interview with the author of the original article, Dr. Christopher Bronk, he downplayed the popular visions of an 'electronic Pearl Harbor' in which critical infrastructure, such as the electrical grid, is knocked out. Such attacks cannot be ruled out entirely, but it is unlikely that a nation-state would launch one because of the catastrophic response it would trigger, he said. Instead, Bronk said, cyberwar will be an effort "to get inside the other guy's decision making process rather than shutting it off entirely."[7] Of course, actions that a nation-state might hesitate to do for fear of retaliation might seem perfectly reasonable to a cyberterrorist who does not have the physical infrastructure of a nation-state to worry about. The factors that might demotivate a nation-state in regard to certain offensive actions may be totally irrelevant to the cyberterrorist. In fact, the cyberterrorist would probably hope that those defending a national infrastructure would believe that certain types of attacks would be less likely because of the potential for retaliation, and would do less to guard against them.

For those in the antiterrorism community, it is self-evident that you do not want any adversary – whether a nation-state or a cyberterrorist deeply embedded over a long time in your systems – able to steal plans and other data, enter false information and cause disruptions to your communications, command and control, logistics and other infrastructures.

[5] Christopher Bronk, "Blown to Bits," *Strategic Studies Quarterly,* Spring 2011.

[6] JaikumarVijayan, "What a Cyberwar with China Might Look Like," *Computerworld*, April 18, 2011.

[7] Ibid.

For the rest of this paper, we will look at the anatomy of an advanced persistent threat attack, and suggest how cyberdefense strategy is evolving from a model focused on perimeter defense to a model focused on more defense-in-depth.

Anatomy of an Advanced Persistent Threat Attack.

The defining feature of an APT attack is persistence. Regardless of other motives – to steal sensitive data, to put tools into place to cause on-demand damage to a network, to be prepared to inject false or misleading information into an information system or whatever operational objective the perpetrator may have (and which can change over time) – the ultimate objective is to gain unauthorized entry into your network and to maintain that access over an extended period. It is not a hit-and-run attack. As the intruder, you donot want to be noticed. You want to fly under the radar and do so for as long as possible.

Unlike more traditional attacks which can be described in standard ways (for example, the SQL injection attack discussed earlier in this paper), the APT perpetrator can choose whatever means of infiltration that will work. For that reason, APTs frequently start with surveillance and intelligence gathering;the perpetrators want to know as much as possible about your network and your information security features as they can find out. They want to know the operating systems you use, the applications and database management systems that have been implemented, and as much as they can learn about employees and the possibility of infiltrating a terrorist sympathizer (someone who is not an actual member of a terrorist cell, but who is willing to act on their behalf – either because they believe in the aims of the terrorists, or they are willing to be employed by them) into your environment.

The more intelligence that can be gathered, the less you are an ‘unknown.’ The information that is collected can be of great value in figuring out how to best gain initial entry into your systems environment and then how to dig in for the long run.

Sometimes there is much more information available than a company may know. For example, a Google or Bing search may turn up information about your organization’s networks in the form of press release from a vendor. We have seen cases in which a vendor white paper described an agency’s key systems architecture (with a network diagram) and a description of the systems environment including operating systems and database management systems in use, and that information was used to enable a successful attack on the system.

For an intruder, time spent researching the target is time well spent. There should be no doubt that those responsible for the intrusion into the US defense systems described by Secretary Lynn did their homework and understood that using a specially-prepared USB device was, for them, an effective way to gain access to the initially targeted network.

Once a would-be APT perpetrator has completed planning, the actual work of the attack can begin.

The following scenario is very typical. While there will be countless variations, there is an anatomy to these attacks.[8]

Many of the attacks that we see start out as an email message. Of course, the email is carefully tailored to make the recipient feel safe in taking the action that the attacker wants. The user could be induced into opening an attachment which contains a computer virus or other form of malware. A user could be induced to click a link to visit a site that will – in addition to whatever else it has in response to the click -- upload malware into the targeted computer. (The automatic uploading of malicious software by simply visiting a suitably-built website is called a “drive-by infection.”)

It could be something other than an email. Perhaps, as in the case discussed by Secretary Lynn, the adversary could use something like a USB device. We have seen cases where an adversary dropped a USB memory device attached to a key ring with a couple of house keys in the parking lot of a building. The perpetrators counted on the fact that a Good Samaritan would find it, and in an attempt to be helpful and find out who lost it plugs it into a computer. Seconds later, the network is infected. Some people believe that APTs always use previously unreported security defects (called “Zero-Day Attacks”) but this is not the case. For high value targets (including sensitive government targets) it is worth it to an attacker to use a zero-day attack – if they have one available. But obtaining a zero-day defect is not easy and can be costly, so attackers will often target a known security defect that may not have been patched, or rely on ‘social engineering’ to get an authorized person to do something foolish.

Once the email attachment is clicked, or the employee visits the linked site, or the USB device is installed, the malware immediately takes control of the employee’s computer, establishing a digital beachhead.

The malware works to establish a connection via the Internet to a server where it can send information and from which it can get instructions (sometimes called a ‘command and control site.’) Once this communication channel is in place, a human attacker uses a ‘back door’ established by the malware to enter the compromised computer. Once inside the compromised system, the attacker can take a stealthy look around, and can typically determine the privileges the machine has on the network, what else is on the network, and what part of the organization the compromised machine belongs to. The key to doing this with a degree of stealth is using tools that are normally on the computer that you are attacking and that are normally used by authorized systems administrators. A systems administrator seeing the use of the ‘netstat’ or ‘nbstat’tools, for example, is unlikely to immediately think of an intrusion, as they are normally used for authorized purposes.

Once the intruder has gained access and looked around, the typical next step is to try to get the passwords of authorized users. Of course, virtually all systems maintain passwords in an encrypted form, but that does not faze the attacker. Using one of a number of hacker tools designed to find and steal encrypted password files. (An example of this is the program ‘pwdump.’) Most of the time, the intruder finds it easier to export the encrypted password list, and process it on a computer – or a network of computers controlled by the attacker.

[8] The anatomy of an attack is in part derived from Christopher Day, “An Approach for the Detection of the Illicit Use of Legitimate Network Access Credentials by an Intruder,” presented at the American Academy of Forensic Sciences 63rd Annual Scientific Meeting, Chicago, IL, February 24, 2011, Session B5.

So now the attacker has the encrypted password file. Assuming it is a strong encryption system, at first glance, it would appear to be virtually impossible to crack the code and get to the original passwords. Unfortunately, this is not the case. Through the use of what are called Rainbow Tables, attackers can often begin identifying passwords within minutes. While the exact way that these work is complex, the idea is simple. Assume for example, that your secret password is "curiosity." When the password is processed through the password encryption system, it comes out as "3v8qr@7dps^4". What if I now take a list of every word in the dictionary, and run it through the same encryption engine used by the system. Somewhere on the resulting list is going to be an entry which says, in effect, "curiosity" = "3v8qr@7dps^4." When I match "3v8qr@7dps^4" from the compromised laptop with the same entry in my table, I know that the matching password must be "curiosity." It is more complex in practice, of course, and there are ways of defending against Rainbow Table attacks, but the reality is that in most cases these defenses arenot in place, and the attacker will quickly succeed in recovering useable passwords. If any of those belongs to a privileged user who has more rights than a normal user (for example a domain administrator) all of those rights are compromised, we have a happy attacker, and the attack continues.

Using the compromised passwords, the attacker moves through the network to access other systems, and to compromise them. Typically, the attacker will choose to compromise a number of network devices and will bring in various tools to create multiple entry points into the network (which the intruders want, because if you find and close their original entry point, they will have many others to permit them to continue to compromise the network). Having multiple entry points also protects against the day when the original user changes their password. That one may not work, but with multiple entry points and compromised passwords, there are always more that will still do the job for the intruder.

When this is accomplished, the intruder can enter the network at will, and if the system provides remote access (using supposedly secure tools like Virtual Private Networks, webmail or enterprise application portals, the intruder can freely use them through their compromised entry points and credentials. This is typically the point when the attackers are secure in their access, and they can focus on their objectives (stealing documents, planting false documents, erasing log files showing what they have been doing, building code structures to render a network unusable or whatever other tasks are set by the attacker's controllers.)

In fact, at this point, it is fair to say that the bad guys are not actually hacking into the system. They have what the systems sees as valid credentials, and they simply log in like any other user to do what they want. It is the adversary's ability to get to the point of masquerading as a valid user that makes APTs so difficult to detect and eliminate.

So now they are in your system and they have probably deployed some additional tools to maintain access. For example, if you find them and close down the malware they are using, they may have planted a little program deep in your system that mostly does nothing. But once every few weeks, it wakes up and checks to see if you are still infected. If you are, it goes back to sleep. If not, it attempts to start the infection chain again – after you believe you have eradicated the problem. Some other malware is designed to re-start itself whenever the computer it is infecting is re-started (These are examples of just how persistent these attacks can be.)

Seeing an ATP in Your Network

Let us assume that for whatever reasons, your perimeter defense did not detect the initial penetration of your network and that no one noticed as the intruders moved through your system to establish a persistent presence. How can you determine if you have been compromised?

While there are no magic answers – new intrusion and new defense techniques will have evolved between the time this is written and the time you read it – but here are some ways that systems security specialists work to detect and defeat these attacks.

- Look for the communication between the malware and those controlling it. This command-and-control traffic can often be recognized either because it is operating through unusual communication ports or because traffic is going to places where you would not expect it to go. Log analysis can help you to see periodic traffic, often indicative of this type of traffic, as the malware 'beacons' or 'calls home' at scheduled intervals. If you detect internal systems sending "here I am" beacons or listening for traffic on unusual ports, is a strong indicator of a persistent attack.
- Look for files and what a security expert could identify as software tools placed in locations that do not make sense relative to the normal operation of the system. Seeing files out of place is a strong indicator that they are being moved as part of a scheme to eventually export them. If you find a cache of executable programs that you do not recognize, particularly in a strange location (for example in the recycle bin) you should be very suspicious. Clearly, having intrusion detection tools and file integrity tools in place in your network is important.
- Using log file analysis (which assumes you have comprehensive logging and that you maintain the logs for a long enough period) you may detect that legitimate credentials are being used in parts of the system where you would not expect them. Activity outside of normal expected ranges should be investigated.
- You can also analyze how valid credentials are being used. Are sessions using valid credentials originating from unexpected places? If an employee is known to be on vacation in the Canary Islands, it would be very suspicious if the person's credentials were being used from somewhere 10,000 miles from the Canary Islands. It is also suspicious when credentials are used at odd times, or where one credential appears to be addressing resources that the person normally would not use. Similarly, if one user credential is sequentially used for sessions one hour apart, but the sessions originate in Washington, Istanbul, Sao Paulo and Vladivostok, you have an intrusion (or an employee who can travel at speeds that Superman would envy.)

Ultimately, most of the analysis that you can do is based on having the right logs. Maintaining Windows event logs, IIS (Internet Information Server) logs, firewall logs, web server logs (Apache logs as an example), Syslogs and Windows RAS (Remote Access Server) logs (and their MAC, Linux, or other operating system equivalents) as well as logs relating to specific applications– and securing them as soon as there is a suspicion of problems (so that they cannot be erased to cover an intruder's tracks) is important, and there should be protocols for locking down systems where necessary. Storage space for logs has become inexpensive. Having logs that are detailed and which are held for a long enough period to be useful is now practical in almost all situations.

Given the potential for an intruder to remove log files to destroy evidence of what was done, consideration should be given to having logs written to locations for which the logging application or system has read-only access. Alternatively, any of a number of log aggregation systems can be used to move logs to a protected environment. Information released about the SONY PlayStation Network intrusion indicates that the intruders erased log files, and that made the investigation more complex.[9]

Toward a Defense in Depth Strategy

We live in a world where the software we use is so complex and consists of so many lines of computer code (sometimes millions of lines of code) and where the pressure to quickly release new versions of programs to satisfy customer or competitive demands is so great, we can no longer assume that the code we run is secure. We know that intruders have also developed techniques that are specifically designed to defeat the controls at the perimeter of our networks. The best firewall will not help if an employee can plug in an infected USB device brought from home. Building a strong perimeter is important, but it isnot enough.

Those organizations that are doing the best job of defending their networks recognize that network defense is a complex and always changing problem. They also realize that implementing a defense-in-depth can be expensive, in terms of technology and of people.

Here are some of the defensive measures to consider. This is not an exhaustive list by any means. And the selection of the right measures for use in a particular situation must flow from the sensitivity of the data, the likelihood that it will be targeted, and the architecture of the network and physical environment within which it is running.

- Control the end-points. You cannot have good security if you do not exercise some control over the equipment your people use. If you provide desktop or laptop computers, as well as smart-phones or tablet computers to your staff, you have a right to control what runs on them. The best advice is to lock them down. Do not let users add on any software without specific permission (based on need and testing the integrity of the proposed software) and donot let them plug in unauthorized USB devices. They will not like you for these decisions, but without them, the job of securing the network becomes much harder. Consider, for example, that even if you lock down the central network, without end-point control, information stored on a laptop computer, for example, can be at risk from malware on the local machine.
- Harden your devices. We see many cases in which an intrusion was made possible by having the wrong settings on a server, router or firewall or even an end-user machine. Organizations like the US National Institute of Standards and Technology provide a number of very useful guides to setting up network devices in a way that improves security.[10]

[9] In a letter sent on May 3, 2011 to the Subcommittee on Commerce, Manufacturing and Trade in response to U.S. Congressional inquiries, Kazuo Hirai, Chairman of the Board of Directors of Sony Computer Entertainment America said "Among other things, the intruders deleted log files in order to hide the extent of their work and activity within the network." (Page 4)

[10] The NIST Security Configuration Checklists can be accessed at no cost at http://checklists.nist.gov.

- Make sure your logs are turned on, are creating detailed records and are saved – securely – for a sufficient period.
- Make sure vulnerable applications are protected by Application Level Firewalls. These programs filter the information that is passed to an application to avoid an intruder's attempt to smuggle in inquiries or commands disguised as regular transactions. Programs such as WebKnight (which is open-source) can be easily installed and configured, and are often a practical solution to protecting an application against SQL injection attacks.
- You should have the appropriate monitoring solutions in place for your sensitive networks. From simple intrusion detection systems to more complex intrusion prevention and data-leakage prevention systems, to more comprehensive packet-capture and traffic monitoring/analysis technologies, it has become vital to design the right level of surveillance into sensitive systems. It's also necessary to have people trained to monitor those security systems, and who have the proper training and experience to interpret alerts, quickly react to problems, and evolve the protection appropriately.
- Keep training your people. While there's no 100% protection against an employee or contractor reacting to a falsified email or other human error, good training can certainly diminish the risk.
- Know your people. Everyone who can access a network with sensitive data should have the appropriate background checks. This not only applies to employees, but to contractors, temporary workers and vendors as well.

Conclusion

There are no easy solutions to the highly sophisticated persistent threat attacks that every organization faces. Terrorist organizations in particular are highly motivated to establish persistent access to the networks of adversaries, targets and those who defend against their attacks. Understanding the problem, and taking the right defensive actions is vital if we're to stay one step ahead of those attacking our networks.

References

Day, Christopher, “An Approach for the Detection of the Illicit Use of Legitimate Network Access Credentials by an Intruder”, presented at the American Academy of Forensic Sciences 63rd Annual Scientific Meeting, Chicago, IL, February 24, 2011, Session B5.

Bronk, Christopher, “Blown to Bits,”*Strategic Studies Quarterly,* Spring 2011,pp. 1-20.

Fogarty, Kevin, “Advanced Persistent Threat is the Best Fake Excuse for Data Breaches” *ITWorld Online*, at www.itworld.comprint/157361(accessed April 27, 2011).

“Highway Robbery,” 60 Minutes, Scott Charney (guest) CBS, WCBS-TV, New York, 1998.

Lynn III, William H., “Defending a New Domain,” *Foreign Affairs*, Vol. 89, No. 5, 2010.

Woodward, Carl, *Obama’s Wars*, Simon & Schuster, New York, NY, USA, 2010.

Vijayan, Jaikumar, “What a Cyberwar with China Might Look Like,”*Computerworld,* April 18, 2011.

Defence Against Terrorism Review
Vol.3, No. 2, Fall 2010, pp. 37-58
Copyright © COE-DAT
ISSN: 1307-9190

Challenges in Developing a Legal Response to Terrorist Use of the Internet

Marco GERCKE
Director, Cybercrime Research Institute, University of Cologne, Germany

Abstract: *Terrorist use of the Internet has been the focus of national governments, as well as regional and international organizations, for several years. Solutions to the phenomenon range from technical protection measures to the development and implementation of legal instruments. This chapter gives an overview of the challenges that go along with the development of legal instruments addressing terrorist use of the Internet and provides an analysis of the concept of the different approaches discussed as the moment.*

Keywords: *Cybercrime, Cyberterrorism, Internet, Terrorism, Legislation,Challenge*

Introduction

Only few decades after its invention, the Internet is widely considered to be a means of communication with great potential for connecting people. The debate about opportunities and threat shows that it has also become a platform for illegal activities including terrorist-related activities.[1] While back in the 1990s the discussion about the use of the network by terrorist organizations focused on network-

[1] United Nations Counter-Terrorism Implementation Task Force (UN CTITF), Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes, 2009, p. 3, available at http://www.un.org/terrorism/pdfs/wg6-internet_rev1.pdf (last visited 6 July 2011).

based attacks against critical infrastructure, such as transportation,[2] energy supply ('cyberterrorism') and the use of information technology in armed conflicts ('cyberwarfare'),[3] this view on terrorist use of the Internet changed after the 9/11 attacks[4] when it was reported[5] that the offenders had used the Internet in the preparation of the attack.[6] Within the debate that ensued, different ways

[2] *See* Marco Gercke, "Cyber-Attacks against Critical Transportation Infrastructure," published in Mete Tahmisoğlu and Çınar Özen, *Transportation Security against Terrorism*, NATO Science for Peace and Security Series, 2009, pp. 151-160.

[3] Marco Gercke, "Cyberterrorism, How Terrorists Use the Internet," *Computer und Recht,* 2007, pp. 62 *et. seq.*

[4] *See* James A. Lewis, "The Internet and Terrorism," *Proceedings of the American Society of International Law*, Vol. 99, pp. 112-115, available at http://www.jstor.org/pss/25659982 (last visited 2 July 2011); James A. Lewis, "Cyber-terrorism and Cybersecurity," Remarks at the Center for Strategic and International Studies, 6 January 2002, available at http://www.csis.org/media/csis/pubs/020106_ cyberterror_cybersecurity.pdf; Gercke, *supra* note 4; Ulrich Sieber and Phillip Brunst, *Cyberterrorism – The Use of the Internet for Terrorist Purposes*, Council of Europe Publications, 2007, available at http://book.coe.int/EN/ficheouvrage.php? PAGEID=36& lang=EN&produit_aliasid=2227 (last visited 6 July 2011); Dorothy Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," in John Arquilla and David Ronfeldt, *Networks & Netwars: The Future of Terror, Crime, and Militancy,* p. 239, available at http://www.rand.org/pubs/monograph_reports/ MR1382/MR1382.ch8.pdf (last visited 4 July 2011); Ayn Embar-Seddon, "Cyberterrorism, Are We Under Siege?," *American Behavioral Scientist,* Vol. 45, No. 3, pp. 1033-1043, available at http://abs.sagepub.com/ content/45/6/1033.abstract (last visited 6 July 2011); John Prados, *America Confronts Terrorism*, Ivan R. Dee, 2002, p. 111 *et seq* (citing United States Department of State, Pattern of Global Terrorism, 2000); Anthony Lake, *Six Nightmares: Real Threats in a Dangerous World and How America Can Meet Them*, Little Brown & Co, 2000, pp. 33 et seq.; Sarah Gordon and Richard Ford, *Cyberterrorism*, Symantec White Paper, undated, available at http://www.symantec.com/avcenter/reference/cyberterrorism.pdf (last visited 11 July 2011; John L. Hennessy, David A. Patterson, and Herbert S. Lin, eds, *Information Technology for Counterterrorism: Immediate Actions and Future Possibilities*, National Academic Press, 2003, pp. 11-14, available at http://www.nap.edu/ catalog.php?record_id=10640 (last visited 11 July 2011); Office of Democratic Institutions and Human Rights, *Comments on Legislative Treatment of Cyberterror in Domestic Law of Individual States*, Organization for Security and Cooperation in Europe, 2007, available at http://www.legislationline.org/upload/lawreviews/93/60/ 7b15d8093cbebb505ecc3b4ef976.pdf.

[5] See Florian Rötzer, "Fahndung im Internet [Search in the Internet], *Telepolis News,* 4 October 2001, available at http://www.heise.de/tp/r4/artikel/9/9717/1. html (last visited 2 July 2011).

[6] The text of the final message was reported to be: "The semester begins in three more weeks. We've obtained 19 confirmations for studies in the faculty of law, the faculty of urban planning, the faculty of fine arts, and the faculty of engineering." The name of the faculties was apparently the code for different targets. For more detail*, see* Gabriel Weimann, "How Modern Terrorism Uses the Internet," *The Journal of International Security Affairs*, Spring 2005, No. 8, available at http://www.securityaffairs.org/ issues/2005/08/weimann.php (last visited 2 July 2011); Timothy L. Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning,'" *Parameters*, Vol. 33, No. 1, Spring 2003, pp. 112–23, available at http://www.iwar.org.uk/cyberterror/resources/ cyberplanning/al-qaeda. htm (last visited 2 July 2011); Tom Zeller, Jr., "On the Open Internet, a Web of Dark Alleys," *The New York Times,* 20 December 2004, available at http://www.nytimes.com/2004/12/20/technology/20covert.html (last visited 2 July 2011).

in which terrorist organizations use the Internet were discovered.[7] The Report of the UN Working Group on Countering the Use of the Internet for Terrorist Purposes lists observed uses to be cyberattacks, fundraising, training, recruitment, secret communication, data mining, propaganda and radicalization.[8]

Addressing those threats encounters the same difficulties as investigating and preventing cybercrime in general but terrorist use of the Internet in specific has unique challenges. The measures discussed to address the issue are just as diverse as the activities themselves. As the Internet is a technical invention, the debate focuses particularly on technical issues such as blocking websites. Yet the debate cannot be reduced to the availability and capability of technical solutions. As has been underlined several times in the Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes, there are various legal aspects that need to be considered within the process of addressing the issue. Apart from fundamental aspects such as how to define 'terrorism' and 'terrorist intent,' it is necessary to address such relevant issues as the protection of human rights, the applicability of investigation instruments and criminal law provisions as well.

General Challenges

The challenges related to the fight against cybercrime in general and terrorist use of the Internet in specific are diverse.[9] One of the main reasons is the fact that the network technology in place addresses technical demands which is not necessary in line with the priorities of the authorities involved in the fight against terrorist use of the Internet.

Number of Users

The popularity of the Internet and its services is growing fast, with over 1.7 billion Internet users worldwide.[10] In 2005, the number of Internet users in developing countries surpassed the number in industrial nations.[11] The increasing number of Internet users is a challenge as the potential number of offenders is increasing as well.[12]

Availability of Tools and Information

Offenders can commit cybercrimes by using software devices that do not require in-depth

[7] For an overview, *see* Sieber and Brunst, *supra* note 5; Gercke, *supra* note 4.

[8] UN CTITF, *supra* note 2, pp. 5-8.

[9] Regarding the challenges, see Marco Gercke, *Understanding Cybercrime: A Guide for Developing Countries*, International Telecommunication Union 2009, p. 65.

[10] For recent statistics, see International Telecommunications Union, "ICT Data and Statistics, at http://www.itu.int/ITU-D/ict/statistics/ (last visited 11 July 2011).

[11] *See* Development Gateway, Special Report on Information Society – Next Steps?, 2005, summary available at http://bytesforall.net/?q=node/12 (last visited 11 July 2011).

[12] See Gercke, *supra* note 11, at p. 65.

technical knowledge, such as software tools[13] designed to locate open ports or break password protection.[14] Due to mirroring techniques and peer-to-peer exchange, it is difficult to limit the widespread availability of such devices[15] that can potentially turn any computer user into a cybercriminal. In addition to software, offenders can use the Internet to find various instructions on how to commit crimes both online and offline. Several reports have emphasized the risk of the use of search engines for illegal purposes.[16] An offender who plans an attack can find detailed information on the Internet that explains how to build a bomb by using only those chemicals that are available in regular supermarkets.[17] Although information like this was available before the Internet was developed, it was much more difficult to get access to that information.

Both technical and legal approaches to address the availability of tools and information are currently being discussed. One example of a technical approach is the limitation of search results by a search engine provider,[18] or restricting the level of details in satellite pictures provided online.[19] The debate about legal responses ranges from criminalization of the production, sale or even possession of tools primarily designed to commit sophisticated computer attacks,[20] to criminalizing the publication of critical information.[21]

[13] Websense, *Security Trends Report: Second Half 2004*, Websense, 2005, p. 11, available at http://aolsearcht12.search.aol.com/aol/search?enabled_terms=&s_it= comsearch50&q=Websense+Security+Trends+Report+2004 (last visited 7 July 2011); United States Government Accounting Office, "Information Security: Computer Controls over Key Treasury Internet Payment System," Report GAO-03-837 GAO, 2003, p. 3, available at http://www.gao.gov/new.items/d03837.pdf (last visited 11 July 2011); Ulrich Sieber, "Focus: The Threat of Cybercrime," *Organised Crime Situation Report 2004*, Council of Europe, 2004, p. 143.

[14] Kelley Ealy, "A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention," SANS Institute, 2003, p. 9, available at http://www32.giac.org/paper/gsec/3055/evolution-hack-attacks-general-overview-types-methods-tools-prevention/105082> (last visited 6 July 2011).

[15] In order to limit the availability of such tools, some countries criminalize the production and offer of such tools. An example of such a provision can be found in the European Convention on Cybercrime, art. 6.

[16] See Yuki Nogguchi, "Search Engines Lift Cover of Privacy," *The Washington Post,* 09 February 2004, available at http://www.msnbc.msn.com/id/4217665/ns/ technology_and_science-washington_post/t/online-search-engines-lift-cover-privacy/ (last visited 6 July 2011).

[17] One example is the Terrorist Handbook – a pdf-document that contains detailed information how to build explosives, rockets and other weapons, available at, e.g., http://www.capricorn.org/~akira/home/terror.html (last visited 6 July 2011).

[18] See testimony of Nicole Wong, Associate General Counsel, Google Inc., Hearing on Making the Internet Safe for Kids, Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, United States House of Representatives, June 27, 2006.

[19] Regarding the related threats, *see* Phillip Brunst, "Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet," in Marianne Wade and Almir Maljevic, *A War on Terror?: The European Stance on a New Threat, Changing Laws and Human Rights Implications,* Springer, 2010, p. 55.

[20] In this context, *see, e.g.,* Council of Europe Convention on Cybercrime, ETS 185, 23 November 2001, [hereinafter Cybercrime Convention], art. 6.

[21] Regarding the criminalization of terrorist related training material see: EU Framework Decision 2008/919/JHA amending Framework Decision 2002/475/JHA on Combating Terrorism, OJ L 330/21, 28 November 2008, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:330:0021:0023:EN:PDF (last visited 14 July 2011).

Transnational Dimensions

The protocols used for Internet data transfers are based on optimal routing if direct links are temporarily blocked.[22] In addition, various popular Internet services used by Internet users worldwide are not provided locally but in one country. As a consequence of both these aspects, many data transfer processes affect more than one country.[23] If offenders and targets are located in different countries, cybercrime investigations need the cooperation of law enforcement agencies in all countries affected.[24] National sovereignty does not permit investigations within the territory of different countries without the permission of local authorities.[25] As a consequence, international cooperation between the different law enforcement agencies involved is required. The formal requirements and time needed to collaborate with foreign law enforcement agencies often hinder investigations,[26] as these often occur within very short time frames. Offenders may deliberately include third countries in their attacks to make investigation more difficult.[27]

The discussion about solutions for the related challenges focuses on two key issues: harmonization of legislation and improvement of international cooperation in criminal matters. The aim of harmonization of legislation is to reach a minimum degree of compatibility of legal approaches. This issue is still very much under discussion as existing international and regional legal frameworks, at the time of this report, do not provide a comprehensive legal framework specifically addressing terrorist use of the Internet. Such an approach can, for example, be found in more recent scientific

[22] The first and still most important communication protocols are Transmission Control Protocol (TCP) and Internet Protocol (IP). For further information, see Andrew Tanenbaum, *Computer Networks,* 4th ed., Prentice Hall, 2002; Douglas Comer, *Internetworking with TCP/IP – Principles, Protocols and Architecture*, 3rd ed., Prentice Hall, 1995.

[23] Regarding the extent of transnational attacks in the most damaging cyberattacks, see Abraham Sofaer and Seymour Goodman, "Cyber Crime and Security – The Transnational Dimension," in Abraham Sofaer and Seymour Goodman, eds, *The Transnational Dimension of Cyber Crime and Terrorism*, Hoover Institution Press, 2001, p. 7.

[24] Regarding the need for international cooperation in the fight against Cybercrime, see Tonya Putnam and David Elliott, "International Responses to Cyber Crime," in Abraham Sofaer and Seymour Goodman, *Transnational Dimension of Cyber Crime and Terrorism,* 2001, pp. 35-66 ; Sofaer and Goodman, *supra* note 24, pp. 1-34.

[25] National Sovereignty is a fundamental principle in International Law. *See* Brad Roth, "State Sovereignty, International Legality, and Moral Disagreement," Paper Presented at the Panel on "Questioning the Aspiration to Global Justice," Annual Meeting of the American Political Science Association, September 2, 2005, p. 1, available at http://www.ihrr.net/download-document/267-state-sovereignty-int-legality-morality-roth-2005?mode=view (last visited 12 July 2011).

[26] Marco Gercke, "The Slow Wake of a Global Approach against Cybercrime," *Computer Law Review International 2006*, No. 5, 2006, p. 142. For examples, *see* Sofaer and Goodman, *supra* note 24, p. 16.

[27] James Lewis, "Computer Espionage, Titan Rain and China," Center for Strategic and International Studies, p. 1, at http://www.csis.org/media/csis/pubs/ 051214_china_titan_rain.pdf (last visited 12 July 2011).

approaches such as the 2009 Draft ITU Cybercrime Legislation Toolkit.[28] Instruments related to the improvement of international cooperation are, for example, the United Nations Convention against Transnational Organized Crime (UNTOC) and the Council of Europe Convention on Cybercrime.

Difficulties in Tracing Offenders

Offenders can hinder investigations (and in particular their identification) by accessing the Internet through public Internet terminals that do not require an identification procedure or by using open wireless networks to hide their identity. While difficulties in identifying Internet users have – similar to secret elections – the potential to support democratic processes, they also go along with fears of abuse by terrorist organizations.

Different legal solutions have been developed.[29] One such example is a legal obligation established in Italy where public Internet access providers are required to identify users before they allow the user to access the service.[30]

Missing Mechanisms of Control

The Internet was originally designed as a military network,[31] based on a decentralized network architecture that sought to preserve the main functionality intact, even when components of the network were attacked. As it was not originally designed to facilitate criminal investigations or to prevent attacks from inside the network, undertaking investigations that require means of control bring unique challenges.[32]

[28] Marco Gercke and Tatiana Tropina, "From Telecommunication Standardisation to Cybercrime Harmonisation? ITU Toolkit for Cybercrime Legislation," *Computer Law Review International 2009*, No. 5, 2009, page 136-140, available at http://cat.inist.fr/?aModele=afficheN&cpsidt=22015168 (last visited 11 July 2011**).**

[29] Gercke, *supra* note 10, Section 6.2.11.

[30] Decree-Law 27 July 2005, No. 144. – Urgent measures for combating international terrorism. For further information on the Decree-Law, see, e.g., InfoDev, "Privacy and Data Retention Policies in Selected Countries," at http://www.ictregulationtoolkit. org/en/PracticeNote.aspx?id=2026 (last visited 14 July 2011).

[31] For a brief history of the Internet, including its military origins, see Barry Leiner, *et al, "*A Brief History of the Internet," Internet Society, at http://www.isoc.org/internet/ history/brief.shtml (last visited 12 July 2011).

[32] Howard Lipson, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues," Report CMU/SEI-2002-SR-009, Carnegie Mellon Software Enginerring Institute, 2002, available at *www. cert.org/archive/pdf/02sr009.pdf* (last visited 12 July 2011).

Several technical solutions, as well as their related legal obligations, to control Internet traffic have been developed and implemented in the last years.[33] Norway,[34] Sweden,[35] Switzerland,[36] United Kingdom,[37] Italy,[38] China,[39] Iran,[40] and Thailand[41] are among those countries that require or encourage

[33] Cormac Callanan, *et al,* "Internet Blocking – Balancing Cybercrime Response in Democratic Societies," Aconite Internet Solutions, 2009 at http://www.aconite.com/ sites/default/files/Internet_blocking_and_Democracy.pdf (last visited 14 July 2011).

[34] "Telenor Group, "Telenor and KRIPOS Introduce Internet Child Pornography Filter," Telenor Press Release, 21 September 2004, available at http://www.telenor.com/en/news-and-media/press-releases/2004/telenor-and-kripos-introduce-internet-child-pornography-filter (last visited 12 July 2011); Richard Clayton, "Failures in a Hybrid Content Blocking System," pp. 1-2, at http://www.cl.cam.ac.uk/~rnc1/ cleanfeed.pdf, (last visited 12 July 2011); Wouter Stol, Filteren van kinderporno op internet [Filtering of child pornography on the Internet], 2008, p. 46 *et seq*., available at wodc.nl/images/1616_volledige_tekst_tcm44-117157.pdf (last visited 14 July 2011); The Cybercrime Convention Committee, Examples of How the Private Sector Has Blocked Child Pornography Sites, Council of Europe, T-CY (2006) 04, p. 3, available at www.coe.int/t/dghl/standardsetting/t-cy/T-CY%20 (2006)%2004%20E.pdf (last visited 14 July 2011).

[35] Swedish Providers are using a tool called "Netclean Pro Active." See product description at http://www.netclean.com/eng/?page_id=20 (last visited 14 July 2011). Telenor Group, "Telenor and Swedish National Criminal Investigation Department to Introduce Internet Child Porn Filter, Telenor Press Release, 17 May 2005, available at: http://press.telenor.com/PR/200505/994781_5.html; Stol, *et al, supra* note 35, p. 59 et seq.; The Cybercrime Convention Committee, *supra* note 35, p. 3; Tom Edwards and Gareth Griffith, "Internet Censorship and Mandatory Filtering," E-Brief 5/08, NSW Parliamentary Library Research Service, Nov. 2008, p. 6, at http://www.parliament. nsw.gov.au/prod/parlment/publications.nsf/0/7F8B9A55E2FC932CA2575030083844A/$File/E%20Brief%20Internet%20Censorship.pdf (last visited 14 July 2011).

[36] Ulrich Sieber and Malaika Nolde, Sperrverfuegungen im Internet [Banning Regulations on the Internet], Duncker & Humblot Gmbh ,2008, p. 55; Christian Schwarzenegger, Sperrverfuegungen gegen Access-Provider in Oliver *Arter* and Florian S. *Jörg,* eds*., Internet-Recht und Electronic Commerce Law,* Stämpfli Verlag, Bern, 2003, p. 250.

[37] Edwards and Griffith, *supra* note 36, p. 4. Stol, *et al, supra* note *35,* p. 64 *et seq*.; The Cybercrime Convention Committee (T-CY), *supra* note 35, p. 3; Marie Eneman, A Critical Study of ISP Filtering of Child Pornography, Paper, 2006, at http://is2.lse.ac.uk/asp/aspecis/20060154.pdf (last visited 14 July 2011).

[38] Ilaria Lonardo, "Italy: Service Provider's Duty to Block Content," *Computer Law Review International 2007*, 2007, p. 89 *et seq*.; Edwards and Griffith, *supra* note 36, p. 6 *et seq*.; Sieber and Nolde, *supra* note 37, p. 54.

[39] Richard Clayton, Stephen Murdoch and Robert Watson, "Ignoring the Great Firewall of China," Privacy Enhancing Technologies: 6th International Workshop, PET 2006, Cambridge, UK, June 28-30, 2006, available at http://www.cl.cam.ac.uk/~rnc1/ ignoring.pdf (last visited 10 July 2011); Andreas Pfitzmann, Stefan Köpsell, and Thomas Kriegelstein, "Sperrverfuegungen gegen Access-Providers: Technisches Gutachten [Blocking Regulations against Service Providers: Technical Advice]," Dresden Technical University, 2008, available at http://www.eco.de/dokumente/ 20080428_technisches_Gutachten_Sperrvervuegungen.pdf (last visited 14 July 2011); Sieber and Nolde, *supra* note 37, p. 53; Stol, *supra* note 35, p. 73.

[40] Sieber and Nolde, *supra* note 37, p. 53; Stol, *supra* note 35, p. 73;

[41] Sieber and Nolde, *supra* note 37, p. 55.

blocking access to illegal content stored outside the country. While this in general seems like proof of the existence of control instruments, the ability of users to circumvent filter technology[42] using encrypted anonymous communication services shows the limitation of such an approach. If access providers block certain websites with illegal content (such as child pornography), customers are generally unable to access those websites.[43] However, the blocking of illegal content can be avoided if customers use an anonymous communication server encrypting communications between them and the central server.

Independence of Location and Presence at the Crime Site

Perpetrators committing Internet-related crimes do not need to be present at the same location as the target. Offenders can therefore act from locations where there is either no effective legislation in place or where such legislation cannot be enforced.[44] Preventing the creation of such 'safe havens' has therefore become a key intention of international approaches in the fight against cybercrime.[45]

[42] Regarding filter obligations/approaches, see Jonathan Zittrain and Benjamin Edelman, "Documentation of Internet Filtering Worldwide," Harvard Law School available at: http://cyber.law.harvard.edu/filtering/; see also Joel Reidenberg, "States and Internet Enforcement," *University of Ottawa Law & Technology Journal,* Vol. 1, No. 213, 2004, page 213 et. seq., available at: http://papers.ssrn.com/sol3/papers. cfm?abstract_id=487965 (last visited 14 July 2011). Regarding the discussion about filtering in different countries, see David Taylor, "Internet Service Providers (ISPs) and Their Responsibility for Content under the New French Legal Regime," *Computer Law & Security Report,* Vol. 20, Issue 4, 2004, pp. 268-272, available at http://www.sciencedirect.com/science/article/pii/S0267364 904000470 (last visited 14 July 2011); European Digital Rights, "Belgium ISP Ordered by the Court to Filter Illicit Content," *EDRi News*, No. 5.14, 18 July 2007, available at http://www.edri.org/ edrigram/number5.14/belgium-isp (last visited 14 July 2011); John Enser, "Illegal Downloads: Belgian Court Orders ISP to Filter," OLSWANG E-Commerce Update, 11.07, p. 7, at http://www.olswang.com/updates/ecom_nov07/ ecom_nov07.pdf (last visited 14 July 2011); Dugie Standeford, "France to Require Internet Service Providers to Filter Infringing Music," *Intellectual Property Watch*, 27 November 2007, available at http://www.ip-watch.org/weblog/index.php?p=842 (last visited 14 July 2011); Gerrit-Jan Zwenne, "Dutch Telecoms Wants to Force Internet Safety Requirements," *World Data Protection Report,* Issue 09/07, 2009 p. 17; International Federation of the Phonographic Industry, "ISPs – Technical Optons for Addressing On-line Copyright Enfringement," IFPI, 2007, available at http://www.eff.org/files/filenode/ effeurope/ifpi_filtering_memo.pdf (discussing the technical options for addressing online copyright infringement)(last visited 15 July 2011). Regarding self-regulatory approaches, see ISPA Code Review, "Self-Regulation of Internet Service Providers," Internet Service Providers' Association, 2002**.**

[43] Callanan, *et al, supra* note 34, p. 40 et seq.

[44] Gercke, *supra* note 10, p. 71.

[45] This issue has been addressed by a number of international organizations. UN General Assembly points out that States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies. UNGA Resolution 55/63, 4 December 2000, available at http://www.unodc.org/pdf/ crime/a_res_55/res5563e.pdf (last visited 15 July 2011). The G8 Ten Point Action Plan highlights that there must be no safe havens for those who abuse information technologies. See BBC, G8 wages war on cyber-crime, BBC News, December 11, 1997, available at http://news.bbc.co.uk/2/hi/science/nature/38009.stm (last visited 15 July 2011).

Automation and Resources

Cybercrime offenders can use automation to scale up their activities. One example of this approach is 'spam.' Offenders can send out billions of unsolicited bulk spam[46] messages by automation within a short time frame.[47] Hacking attacks are another example of the use of automation.[48] Up to 80 million hacking attacks every day[49] are a result of the availability of software tools[50] that can attack thousands of computer systems in the span of just hours.[51] By automating these processes, offenders can profit greatly by designing scams that are based on a high number of offenses with a relatively low loss for each victim.[52] The automation is not the only problem that causes difficulties in investigating and preventing such attacks; offenders can use 'botnets' to commit powerful attacks such as the attack against computer systems in Estonia.[53] Analysis of that attack suggests that it was committed by thousands of computers within a 'botnet'[54] – a group of compromised computers

[46] The term 'spam' describes the process of sending out unsolicited bulk messages. For a more precise definition, see International Telecommunication Union, "ITU Survey on Anti-Spam Legislation Worldwide 2005," ITU, p. 5, available at http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf (last visited 15 July 2011).

[47] For more details on the automation of spam mails and the challenges for law enforcement agencies, see Terrence Berg, "The Changing Face of Cybercrime – New Internet Threats Create Challenges to Law Enforcement Agencies, *Michigan Law Journal*, Vol. 86, No. 6, June 2007, p. 21, available at http://www.michbar.org/journal/pdf/pdf4article 1163.pdf (last visited 12 July 2011).

[48] Kelley Ealy, "A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention," Sans Institute, 2003, p. 9 *et seq*., available at http://www32.giac.org/paper/gsec/3055/evolution-hack-attacks-general-overview-types-methods-tools-prevention/105082 (last visited 14 July 2011).

[49] The online-community HackerWatch publishes regular reports on hacking attacks. Based on their sources, more than 250 million incidents were reported in only one month (August 2007). See McAffe, "HackerWatch," at http://www.hackerwatch.org (last visited 15 July 2011).

[50] Regarding the distribution of hacking tools, see CC Cert, "Overview of Attack Trends," Carnegie Mellon University 2002, p. 1, at http://www.arcert.gov.ar/webs/ textos/attack_trends.pdf (last visited 15 July 2011).

[51] See *ibid.*

[52] According to figures for 2008-2010 from the U.S. Federal Trade Commission (FTC), more than 80% of all fraud complaints reported related to an amount paid of 1000 USD or less. See FTC, Consumer Fraud and Identity Theft Complaint Data – January – December 2010, Federal Trade Commission, March 2011, available at http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2010.pdf (last visited 15 July 2011).

[53] Regarding the attacks, see James Lewis, "Cyber Attacks Explained," Center for Strategic and International Studies, 2007, available at http://www.comw.org/ rma/fulltext/070615lewis.pdf (last visited 15 July 2011); see also "A Cyber-riot," *The Economist*, 10 May 2007, available at http://www.economist.com/world/europe/PrinterFriendly.cfm?story_id=9163598 (last visited 15 July 2011); Mark Landler and John Markoff, "Digital Fears Emerge After Data Siege in Estonia," *The New York Times*, 29 May 2007, available at http://www.nytimes.com/2007/ 05/29/technology/29estonia.html (last visited 15 July 2011).

[54] See Beatrice Toth, "Estonia under Cyber Attack," HUN-Cert, at http://www.cert.hu/dmdocuments/Estonia_attack2.pdf (last visited 14 July 2011).

running programs under external control.[55] Over the last few years, botnets have become a serious risk for cybersecurity.[56] The size of a botnet can vary from a few computers to more than a million computers.[57]

Both technical and legal solutions can address the issue. One focus is on a technical approach,[58] but the success of the recent takedown of the Waledac network in early 2010, which included court action, highlighted the importance of legal measures as part of the strategy.[59]

Encryption Technology

Another factor that can complicate the investigation of cybercrime is encryption technology,[60] which protects information from access by unauthorized people and is a key technical solution in

[55] See Nicholas Ianelli and Aaron Hackworth, "Botnets as a Vehicle for Online Crime," CERT Coordination Center, 2005, p. 3, available at www.cert.org/archive/pdf/ Botnets.pdf (last visited 14 July 2011).

[56] See General Accounting Office, "Emerging Cybersecurity Issues Threaten Federal Information Systems," Report GAO-05-231, 2005, available at http://www.gao.gov/new.items/d05231.pdf (last visited 15 July 2011).

[57] Gregg Keizer, "Dutch Botnet Suspects Ran 1.5 Million Machines," *TechWeb News,* 21 October 2005.

[58] Felix Leder, Tillmann Werner, and Peter Martini, "Proactive Botnet Countermeasures – An Offensive Approach," *Proceedings of the 1st CCDCOE Conference on Cyber Warfare, Tallinn, Estonia, 2009, available at http://www.ccdcoe.org/cyberwarfare/images/146.pdf (last visted 15 July 2011);* Guofei Gu, Junjie Zhang, and Wenke Lee, "BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic", Proceedings of the 15th Annual Network and Distributed System Security Symposium (NDSS'08), 2008, available at http://faculty.cs.tamu.edu/guofei/paper/Gu_NDSS08_botSniffer.pdf (last visited 15 July 2011); Guofei Gu, *et al,* "Active Botnet Probing to Identify Obscure Command and Control Channels," in Proceedings of 2009 Annual Computer Security Applications Conference (ACSAC'09), 2009, available at http://www.cc.gatech.edu/pixi/pubs/Stoll-ACSAC09.pdf (last visited 15 July 2011).

[59] Regarding this approach, see Sakthi Prasad, "Microsoft Wins Court Approval to Topple Botnet," Reuters, 25 February 2010, available at http://www.reuters.com/ article/2010/02/25/us-microsoft-idUSTRE61O1RG20100225 (last visited 15 July 2011).

[60] Regarding the impact on computer forensic and criminal investigations, see Ewa Huebner, Derek Bem and Oscar Bem, "Computer Forensics – Past, Present And Future," *Information Security Technical Report,* Vol. 8, No. 2, pp. 32-46, available at http://www.mendeley.com/research/forensics-past-present-future-2/ (last visited 15 July 2011).

the fight against cybercrime.[61] Like anonymity, encryption is not new,[62] but computer technology has transformed the field. It is now possible to encrypt computer data with the click of a mouse, making it difficult for law enforcement agencies to break the encryption and access the data.[63] It is uncertain to what extent offenders already use encryption technology to mask their activities but it has been reported that terrorists are using encryption technology.[64]

[61] With regard to the importance of encryption technology see Directorate for Science Technology and Industry, Report on Background and Issues of Cryptography Policy, Organization for Economic Cooperation and Development, 2007, available at http://www.oecd.org/document/36/0,3746,en_2649_34255_1814820_1_1_1_1,00.html (last visited 15 July 2011). The importance of encryption is further highlighted by the fact that 74 per cent of respondents to the 2006 E-Crime Watch Survey mentioned encryption technology as one of the most efficient e-crime fight technologies. See CSO Magazine, *et al,* "2006 E-Crime Watch Survey," Press Release, 6 September 2006, p. 1, available at www.cert.org/archive/pdf/ecrimesurvey06.pdf (last visited 15 July 2011).

[62] See, ***e.g.,*** Simon Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, Doubleday, 1999; Alexander D'Agapeyeff*, Codes and Ciphers – A History of Cryptography,* Hesperides Press 2006.

[63] Regarding the consequences for law enforcement, Dorothy Denning has observed that:

> The widespread availability of unbreakable encryption coupled with anonymous services could lead to a situation where practically all communications are immune from lawful interception (wiretaps) and documents from lawful search and seizure, and where all electronic transactions are beyond the reach of any government regulation or oversight. The consequences of this to public safety and social and economic stability could be devastating

Dorothy Denning, "The Future of Cryptography," Georgetown University, 6 January 1996, available at http://www.cosc.georgetown.edu/~denning/crypto/Future.html (last visited 15 July 2011). Regarding practical approaches to recovering encrypted evidence see Eoghan *Casey,* "Practical Approaches to Recovering Encrypted Digital Evidence," *International Journal of Digital Evidence*, Vol. 1, No. 3, 2002, available at http://www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf (last visited 15 July 2011).

[64] Regarding the use of cryptography by terrorists, see Michele Zanini and Sean Edwards, "The Networking of Terror in the Information Age," in John Arquilla and David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy*, Rand Publishing, 2001, p. 37; Kenneth Flamm, "Cyber Terrorism and Information Warfare: Academic Perspectives: Cryptography," in Yonah Alexander and Michael S. Swetnam, eds, *Cyber Terrorism and Information Warfare*, Transnational Publishers, Inc., 2001, available at http://www.terrorismcentral.com/Library/Teasers/Flamm.html (last visited 15 July 2011).

Different legal solutions have been discussed[65] to address the issue.[66] The most common solutions are authorization to break encryption,[67] limitation of the performance of encryption software by restricting the key length,[68] creation of an obligation to establish a key escrow system or key recovery procedure for strong encryption products,[69] and the use of a production order.[70] The implementation of such instruments was discussed at the 1997 G-8 Meeting in Denver.[71] A number

[65] The issue has been addressed by the Council of Europe: "Measures should be considered to minimise the negative effects of the use of cryptography on the investigation of criminal offenses, without affecting its legitimate use more than is strictly necessary." Committee of Ministers, "Recommendation No. R (95) of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected with Information Technology, 11 September 1995, para. 14, available at https://wcd.coe.int/wcd/com.instranet.InstraServlet?command=com.instranet.Cmd BlobGet&InstranetImage=536686&SecMode=1&DocId=528034&Usage=2 (last visited 14 July 2011); see Denver Summit of the Eight, "Counterterrorism," *Foreign Ministers' Progress Report,* G-8 Centre, 21 June 1997, para. 26, available at http://www.g7.utoronto.ca/summit/1997denver/ formin.htm (last visited 15 July 2011).

[66] See Bert-Japp Koops, *The Crypto Controversy: A Key Conflict in the Information Society*, Kluwer Law International, 1998.

[67] "National cryptography policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible." OECD, Guidelines for Cryptography Policy, adopted 27 March 1997, Principle 6,available at http://www.oecd.org/document/11/0,3343,en_2649_34255_1814731_1_1_1_1,00 .html (last visited 15 July 2011).

[68] Export limitations for encryption software that is able process strong keys are not designed to facilitate the work of law enforcement agencies in the country. The intention of such regulations is to prevent the export of the technology outside the country. For detailed information on import and export restrictions with regard to encryption technology, see Bert-Jaap koops, "Crypto Law Survey," July 2010, at http://rechten.uvt.nl/koops/cryptolaw/index.htm (last visited 15 July 2011).

[69] See James Lewis, "Encryption Again," Center for Strategic and International Studies, 1 October 2001, available at http://www.csis.org/media/csis/pubs/011001_encryption_ again.pdf (last visited 15 July 2011).

[70] The term describes the obligation to disclose a key used to encrypt data. See Malte Diehl, "Kryptographiegesetzgebung im Wandel: Von begrenzten Schlüssellängen zur Schlüsselherausgabe [Cryptography Legislation in Change: From Limited Key Lengths to Key Disclosure]," *Datenschutz und Datensicherheit [Data Protection and Data Security],* Vol. 4., 2008, p. 243-247.

[71] The final text on this issue was:

> To counter, *inter alia*, the use of strong encryption by terrorists, we have endorsed acceleration of consultations and adoption of the OECD guidelines for cryptography policy and invited all states to develop national policies on encryption, including key, management. which may allow, consistent with these guidelines. lawful government access to prevent and investigate acts of terrorism and to find a mechanism to cooperate internationally in implementing such policies

Denver Summit of the Eight, "Counterterrorism," *Foreign Ministers' Progress Report,* G-8 Centre, 21 June 1997, para. 26, available at http://www.g7.utoronto.ca/summit/ 1997 denver/ formin.htm (last visited 15 July 2011).

of countries have implemented such obligations;[72] examples are Section 69 of India's Information Technology Act 2000[73] and Section 49 of the United Kingdom's Regulation of Investigatory Powers Act 2000.[74]

[72] See, e.g. Antigua and Barbuda, Computer Misuse Bill 2006, Art. 25, available at http://www.laws.gov.ag/bills/2006/computer-misuse-bill-2006.pdf (last visited 15 July 2011); Australia, Cybercrime Act, Art. 12, available at http://www.cybercrimelaw.net/Australia.html (last visited 15 July 2011); Belgium, Wet van 28 november 2000 inzake informaticacriminaliteit, Art. 9 and Code of Criminal Procedure, Art. 88, available at http://193.191.208.6/cgi_loi/loi_N.pl?cn= 2000112834 (last visited 15 July 2011); France, Loi pour la confiance dans l'économie numérique, Sec. 4, Art. 37, available at http://www.legifrance.gouv.fr/html/actualite/ actualite_legislative/decrets_application/2004-575.htm (last visited 15 July 2011); United Kingdom, Regulation of Investigatory Powers Act 2000, Art. 49, available at http://www.legislation.gov.uk/ukpga/2000/23/contents (last visited 15 July 2011); India, The Information Technology Act, 2000, Art. 69, available at: http://www.legalserviceindia.com/cyber/itact.html (last visited 15 July 2011); Ireland, Electronic Commerce Act, 2000, Art. 27, available at http://www.oireachtas.ie/ documents/bills28/acts/2000/a2700.pdf (last visited 15 July 2011); Malaysia, Communications and Multimedia Act, Section 249, available at http://www.msc.com.my/cyberlaws/act_communications.asp (last visited 15 July 2011); Morocco, Loi relative a l'echange electronique de donnees juridiques, Chapter. III, available at http://droitmaroc.wordpress.com/2008/01/29/loi-n%C2%B0-53-05-relative-a-lechange-electronique-de-donnees-juridiques-integrale/ (last visited 15 July 2011); Netherlands, Wet op de inlichtingen en veiligheidsdiensten 2002, Art. 89, available at http://www.st-ab.nl/wetten/0662_Wet_op_de_inlichtingen-_en_veiligheids diensten_2002.htm (last visited 15 July 2011); South Africa, Regulation of Interception of Communications and Provisions of Communications-Related Information Act, Art. 21, available at http://www.info.gov.za/gazette/acts/2002/a70-02.pdf (last visited 15 July 2011); Trinidad and Tobago, The Computer Misuse Bill 2000, Art. 16, available at http://www.ttcsweb.org/articles/computer-laws/computer-misuse-act-2000/compbill.pdf (last visited 15 July 2011).

[73] An example can be found in Indian law:

> Directions of Controller to a subscriber to extend facilities to decrypt information. (1) If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign Stales or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource. (2) The subscriber or any person in-charge of the computer resource shall, when called upon by any agency which has been directed under sub-section (1), extend all facilities and technical assistance to decrypt the information.

For more information about the Indian Information Technology Act 2000, see Pavan Duggal, "India's Information Technology Act, 2000," available at http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan002090.pdf (last visited 15 July 2011).

[74] For general information on the Act, see Ian Brown and Brian Gladman, "The Regulation of Investigatory Powers Bill - Technically Inept: Ineffective Against Criminals While Undermining the Privacy, Safety and Security of Honest Citizens and Businesses," Foundation for Information Policy Research, undated, available at http://www.fipr.org/rip/RIPcountermeasures.htm (last visited 15 July 2011); Mark Ward, "Campaigners Hit by Decryption Law," *BBC News*, 20 November 2007, available at http://news.bbc.co.uk/2/hi/technology/7102180.stm; Jody R. Westby, "International Guide to Combating Cybercrime," American Bar Association, 2003, p. 32.

Failure of Traditional Investigation Instruments

An effective campaign against terrorist use of the Internet requires Internet-specific tools and instruments that enable the appropriate authorities to carry out investigations.[75] In this context, measures that are necessary to identify the offender and collect the evidence required for any criminal proceedings are especially needed.[76] These measures can often be the same used in traditional terrorist investigations that do not involve computer technology, but in a growing number of Internet-related cases, traditional investigation instruments are not sufficient to identify an offender. One example is the interception of Voice-over-IP (VoIP) communications.[77] In the last few decades, States have developed investigation instruments – such as wiretapping – that enable the interception of landline as well a mobile phone communications.[78] The interception of traditional voice calls is usually carried out through telecommunications providers.[79] Applying the same principle to VoIP, law enforcement agencies would operate through ISPs and service providers supplying VoIP services.

[75] This was as well highlighted by the drafters of the Council of Europe Convention on Cybercrime that contains a set of essential investigation instruments. The drafters of the report pointed out that not only must substantive criminal law keep abreast of these new abuses, but so must criminal procedural law and investigative techniques. See "Explanatory Report to the Council of Europe Convention on Cybercrime," Chap. 2, Sec. 1, 8 November 2001, available at http://conventions.coe.int/treaty/en/reports/ html/185.htm (last visited 16 July 2011).

[76] Regarding user-based approaches in the fight against cybercrime, see Stefan Gorling, "The Myth of User Education," Proceedings of the 16th Virus Bulletin International Conference, 2006, available at http://ssrn.com/abstract=938695 (last visited 15 July 2011. Commented Jean-Pierre Chevenement, French Minister of Interior, at the G8 Cybercrime Conference in Paris in 2000: "More broadly, we have to educate users. They must all understand what they can and can't do on the Internet and be warned of the potential dangers. As use of the Internet grows, we'll naturally have to step up our efforts in this respect." Opening speech of Jean-Pierre Chevenement, French Minister of Interior, G8 Cybercrime Conference, 17 May 2000.

[77] The term Voice over Internet Protocol (VoIP) is use to describe the transmission technology for delivering voice communications by using packet-switched networks and related protocols. See Richard Swale, *Voice Over IP: Systems and Solutions,* The Institution of Engineering and Technology, 2001; Uyless Black, *Voice Over IP*, 3rd ed., Prentice Hall, 2001.

[78] Regarding the importance of interception and the technical solutions, see Balamurugan Karpagavinayagam, Radu State and Olivier Festor, "Monitoring Architecture for Lawful Interception in VoIP Networks," in *ICIMP '07, Proceedings of the Second International Conference on Internet Monitoring and Protection,* IEEE Computer Society, 2007, available at http://hal.inria.fr/docs/00/16/44/20/PDF/ Monitoring_ Architecture_for_Lawful_Interception_in_VoIP_Networks.pdf(last visited 14 July 2011). Regarding the challenges related to interception of data communication, see Ioannis Chochliouros, Anastasia Spiliopoulou, and Stergios Chochliouros, "Measures for Ensuring Data Protection and Citizen Privacy Against the Threat of Crime and Terrorism: The European Response," in Lech Janczewski and Andrew Colarik, *Cyber Warfare and Cyber Terrorism*, 2007, p. 424.

[79] Regarding the differences between PSTN and VoIP communication, see Jan Seedorf, "Lawful Interception in P2P-Based VoIP Systems," in Henning Schulzrinne, Radu State and Saverio Niccolini, eds., *Principles, Systems and Applications of IP Telecommunication. Services and Security for Next Generation Networks,* Springer, 2008, pp. 217-235.

However, if the service is based on peer-to-peer technology, service providers may generally be unable to intercept communications, since the necessary data is transferred directly between the communicating parties.[80]

Application of Traditional Instruments or Development of New Instruments

It is possible to divide into three categories the different approaches that are used by countries to address the specific challenges of terrorist use of the Internet.

Application of Existing Cybercrime Legislation

Some countries are using existing cybercrime legislation that was developed to cover non-terrorist-related acts to criminalize terrorist use of the Internet. There are three aspects that need to be taken into consideration when used in this context.

Substantive criminal law provisions that were implemented to cover non-terrorist-related acts such as data interference[81] or system interference[82] might be applicable in terrorist-related cases – but very often the range for sentencing is less than what terrorist-specific legislation would allow. Depending on the dogmatic structure of procedural law, this could influence the ability to use sophisticated investigation instruments that are restricted to terrorist or organized crime-related investigation.

The application of investigation tools specific to cybercrime, such as the expedited preservation of computer data,[83] for terrorist use of the Internet is often not controversial since most countries do not limit the application of these tolls to 'traditional' cybercrime offenses but any offense involving computer data.

Regional instruments developed to address the challenge of cybercrime but not specifically to terrorist use of the Internet often contain exemptions for international cooperation regarding political offenses. One example is contained in Article 27 of the Council of Europe Convention on Cybercrime; there a provision that authorizes parties to the Convention to refuse assistance in a mutual assistance request if the request concerns an offense which the Requested Party considers to

[80] Regarding the interception of VoIP by law enforcement agencies, see Bellovin, *et al*, "Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP," Information Technology Association of America, 13 June 2006, available at https://www.cs.columbia.edu/~smb/papers/CALEAVOI Preport.pdf (last visited 15 July 2011); Matthew Simon and Jill Slay, "Voice over IP: Forensic Computing Implications," Proceedings of the 4th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 4th 2006; Seedorf, *supra* note 80.

[81] *See, e.g.*, Convention on Cybercrime, art. 4.

[82] *See id.,* art. 5.

[83] *Id.,* art. 16.

be a political offense or an offense connected with a political offense.[84] As this is often the case when it comes to terrorist use of the Internet, such an approach can hinder the investigation. Therefore, terrorist-specific legal frameworks, such as the Council of Europe Convention on the Prevention of Terrorism of 2005, contain an exclusion from the application of political exception clause in Article 20 for counterterrorist investigations.[85]

Application of Existing (Non-Internet Specific) Terrorism Legislation

Some countries are using existing terrorism legislation to criminalize and prosecute terrorist use of the Internet. One example of a traditional instrument is the Council of Europe Convention on the Prevention of Terrorism from 2005 that was mentioned above. The Convention defines several offenses such as public provocation to commit a terrorist offense[86] and the recruitment for terrorism[87] but does not, for example, contain provisions criminalizing terrorist-related attacks against computer systems. Furthermore, the Convention does not contain procedural instruments; this is a shortfall, especially with regard to the investigation of Internet-related offenses, because specific procedural

[84] The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

a) the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b) it considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.

[85] Article 20 – Exclusion of the political exception clause

1 None of the offences referred to in Articles 5 to 7 and 9 of this Convention, shall be regarded, for the purposes of extradition or mutual legal assistance, as a political offence, an offence connected with a political offence, or as an offence inspired by political motives. Accordingly, a request for extradition or for mutual legal assistance based on such an offence may not be refused on the sole ground that it concerns a political offence or an offence connected with a political offence or an offence inspired by political motives.

[…]

[86] Article 5 – Public provocation to commit a terrorist offence

1. For the purposes of this Convention, public provocation to commit a terrorist offence means the distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of a terrorist offence, where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed.

2 . Each Party shall adopt such measures as may be necessary to establish public provocation to commit a terrorist offence, as defined in paragraph 1, when committed unlawfully and intentionally, as a criminal offence under its domestic law.

[87] Article 6 – Recruitment for terrorism

1. For the purposes of this Convention, recruitment for terrorism means to solicit another person to commit or participate in the commission of a terrorist offence, or to join an association or group, for the purpose of contributing to the commission of one or more terrorist offences by the association or the group.

2. Each Party shall adopt such measures as may be necessary to establish recruitment for terrorism, as defined in paragraph 1, when committed unlawfully and intentionally, as a criminal offence under its domestic law.

instruments are required. Identifying an offender who has incited terrorism using websites requires sophisticated instruments such as the expedited preservation of traffic data.

Development of Pecific Legislation Dealing with Terrorist Use of the Internet

Another approach has been the development of specific legislation addressing terrorist use of the Internet. One example is Section 4f of the Draft ITU Cybercrime Legislation Toolkit. The International Telecommunication Union (ITU) is the UN organization that has the most responsibility for practical aspects of cybersecurity.[88] The aim[89] of the Draft Toolkit is to give countries the ability to use sample language and reference material in the process of developing national cybercrime legislation that can assist, according to the Toolkit's developers, the "establishment of harmonized cybercrime laws and procedural rules."[90] The Toolkit was developed by the American Bar Association based on a 'comprehensive analysis' of the Council of Europe (CoE) Convention on Cybercrime and the cybercrime legislation of developed countries. It aims to be a fundamental resource for legislators, policy experts, and industry representatives to provide them with the pattern for the development of the consistent cybercrime legislation. In addition to traditional approaches, the Toolkit contains several specific terrorist-related offences.[91] It contains several provisions that specifically criminalize terrorist-related computer crimes.

Conclusion

Although the legal community has started to address the problem of terrorist use of the Internet, either through specifically-targeted legislation or new uses of broader criminal legislation, there are still significant gaps in the legal framework that need to be addressed. The closer that national provisions are to one another, the easier and more effective this fight will be.

[88] *See* Paul Cornish, *Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks,* Directorate General External Policies of the Union, European Parliament, 2009, p. 17 available at http://www.isis-europe.org/pdf/2009_artrel_ 247_09-02-epstudy-cyberterrorism.pdf (last visited 2 July 2011).

[89] For more information, *see* Gercke and Tropina, *supra* note 29.

[90] ICT Applications and Cybersecurity Division, "ITU Toolkit for Cybercrime Legislation," International Telecommunication Union, Draft February 2010, p. 8, available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation. pdf (last visited 15 July 2011).

[91] For example, "Unauthorized Access for Purposes of Terrorism" (Sec. 2d), "Unauthorized Access to or Acquisition of Computer Programs or Data for Purposes of Terrorism" (Sec. 3f), "Intent to Cause Interference or Disruption for Purposes of Terrorism" (Sec. 4f), and Intent to Furtherance of Terrorism (Sec. 6h). *Ibid.*

References

BBC, "G8 Wages War on Cyber-crime, BBC News, December 11, 1997.

Bellovin, Steven, *et al*, "Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP," Information Technology Association of America, 13 June 2006.

Berg, Terrence, "The Changing Face of Cybercrime – New Internet Threats Create Challenges to Law Enforcement Agencies," *Michigan Law Journal*, Vol. 86, No. 6, June 2007.

Black, Uyless, *Voice Over IP*, 3rd ed., Prentice Hall, 2001.

Brown, Ian, and Brian Gladman, "The Regulation of Investigatory Powers Bill - Technically Inept: Ineffective Against Criminals While Undermining the Privacy, Safety and Security of Honest Citizens and Businesses," Foundation for Information Policy Research, undated.

Brunst, Phillip, "Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet," in Marianne Wade and Almir Maljevic, *A War on Terror?: The European Stance on a New Threat, Changing Laws and Human Rights Implications*, Springer, 2010.

Casey, Eoghan, "Practical Approaches to Recovering Encrypted Digital Evidence," *International Journal of Digital Evidence*, Vol. 1, No. 3, 2002.

Chochliouros, Ioannis, Anastasia Spiliopoulou, and Stergios Chochliouros, "Measures for Ensuring Data Protection and Citizen Privacy Against the Threat of Crime and Terrorism: The European Response," in Lech Janczewski and Andrew Colarik, *Cyber Warfare and Cyber Terrorism*, 2007.

Clayton, Richard, Stephen Murdoch and Robert Watson, "Ignoring the Great Firewall of China," Privacy Enhancing Technologies: 6th International Workshop, PET 2006, Cambridge, UK, June 28-30, 2006.

Comer, Douglas, *Internetworking with TCP/IP – Principles, Protocols and Architecture*, 3rd ed., Prentice Hall, 1995.

Cornish, Paul, *Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks*, Directorate General External Policies of the Union, European Parliament, 2009,

D'Agapeyeff, Alexander, *Codes and Ciphers – A History of Cryptography*, Hesperides Press 2006.

Denning, Dorothy, "The Future of Cryptography," Georgetown University, 6 January 1996.

Denning, Dorothy, "Activism, Hacktivism, and Cyberterrorism: the Internet as a Tool for Influencing Foreign Policy," in John Arquilla and David Ronfeldt, *Networks & Netwars: The Future of Terror, Crime, and Militancy*, Rand Publishing, 2001.

Diehl, Malte, Kryptographiegesetzgebung im Wandel: Von begrenzten Schlüssellängen zur Schlüsselherausgabe, *Datenschutz und Datensicherheit*, Vol. 4, 2008, p. 243-247.

Ealy, Kelley, "A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention," Sans Institute, 2003.

Economist, "A Cyber-riot," *The Economist*, 10 May 2007.

Edwards, Tom, and Gareth Griffith, "Internet Censorship and Mandatory Filtering," E-Brief 5/08, NSW Parliamentary Library Research Service, November 2008.

Embar-Seddon, Ayn, "Cyberterrorism, Are We Under Siege?," *American Behavioral Scientist,* Vol. 45, No. 3, pp. 1033-1043.

European Digital Rights, "Belgium ISP Ordered by the Court to Filter Illicit Content," EDRi News, No. 5.14, 18 July 2007.

Flamm, Kenneth, "Cyber Terrorism and Information Warfare: Academic Perspectives: Cryptography," in Yonah Alexander and Michael S. Swetnam, eds, *Cyber Terrorism and Information Warfare,* Transnational Publishers, Inc., 2001.

Gercke, Marco, The Slow Wake of a Global Approach against Cybercrime, *Computer Law Review International 2006*, No. 5, 2006.

Gercke, Marco, "Cyberterrorism, How Terrorists Use the Internet," *Computer und Recht,* 2007, pp. 62 *et seq*.

Gercke, Marco, *Understanding Cybercrime: A Guide for Developing Countries,* International Telecommunication Union 2009.

Gercke, Marco, "Cyber-Attacks against Critical Transportation Infrastructure," published in Mete Tahmisoğlu and Çınar Özen, *Transportation Security against Terrorism*, NATO Science for Peace and Security Series, 2009, pp. 151-160.

Gercke, Marco, and Tatiana Tropina, "From Telecommunication Standardisation to Cybercrime Harmonisation? ITU Toolkit for Cybercrime Legislation," *Computer Law Review International 2009*, No. 5, 2009, page 136-140.

Gorling, Stefan, "The Myth of User Education," Proceedings of the 16th Virus Bulletin International Conference, 2006.

Gu, Guofei, Junjie Zhang, and Wenke Lee, "BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic," Proceedings of the 15th Annual Network and Distributed System Security Symposium (NDSS'08), 2008.

Gu, Guofei, *et al,* "Active Botnet Probing to Identify Obscure Command and Control Channels," in Proceedings of 2009 Annual Computer Security Applications Conference (ACSAC'09), 2009.

Hennessy, John, David A. Patterson, and Herbert S. Lin, eds, *Information Technology for Counterterrorism: Immediate Actions and Future Possibilities*, National Academic Press, 2003.

Huebner, Ewa, Derek Bem and Oscar Bem, Computer Forensics – Past, Present And Future, Information Security Technical Report, Vol. 8, No. 2, pp. 32-46.

Ianelli, Nicholas, and Aaron Hackworth, "Botnets as a Vehicle for Online Crime," CERT Coordination Center, 2005.

International Federation of the Phonographic Industry, "ISPs – Technical Optons for Addressing On-line Copyright Enfringement," IFPI, 2007.

ICT Applications and Cybersecurity Division, “ITU Toolkit for Cybercrime Legislation,” International Telecommunication Union, Draft February 2010.

Karpagavinayagam, Balamurugan, Radu State and Olivier Festor, “Monitoring Architecture for Lawful Interception in VoIP Networks,” in *ICIMP ‘07,* Proceedings of the Second International Conference on Internet Monitoring and Protection, IEEE Computer Society, 2007.

Keizer, Gregg, “Dutch Botnet Suspects Ran 1.5 Million Machines,” *TechWeb News*, 21 October 2005.

Koops, Bert-Jaap, *The Crypto Controversy: A Key Conflict in the Information Society*, Kluwer Law International, 1998.

Lake, Anthony, *Six Nightmares: Real Threats in a Dangerous World and How America Can Meet Them*, Little Brown & Co, 2000.

Landler, Mark, and John Markoff, “Digital Fears Emerge After Data Siege in Estonia,” *The New York Times*, 29 May 2007.

Leder, Felix, Tillmann Werner, and Peter Martini, “Proactive Botnet Countermeasures – An Offensive Approach,” *Proceedings of the 1st CCDCOE Conference on Cyber Warfare, Tallinn, Estonia, 2009.*

Lewis, James, “Encryption Again,” Center for Strategic and International Studies, 1 October 2001.

Lewis, James, “Cyber-terrorism and Cybersecurity,” Remarks at the Center for Strategic and International Studies, 6 January 2002.

Lewis, James, “The Internet and Terrorism,” *Proceedings of the American Society of International Law*, Vol. 99, 2005, pp. 112-115.

Lewis, James, “Computer Espionage, Titan Rain and China,” Center for Strategic and International Studies, 2005.

Lewis, James, “Cyber Attacks Explained,” Center for Strategic and International Studies, 2007.

Lipson, Howard, “Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues,” Report CMU/SEI-2002-SR-009, Carnegie Mellon Software Engineering Institute, 2002.

Lonardo, Ilaria, Italy: Service Provider’s Duty to Block Content,” *Computer Law Review International 2007*, 2007.

Nogguchi, Yuki, “Search Engines Lift Cover of Privacy,” *The Washington Post*, 09 February 2004.

Pfitzmann, Andreas, Stefan Köpsell, and Thomas Kriegelstein, “Sperrverfuegungen gegen Access-Providers: Technisches Gutachten ,” Dresden Technical University, 2008.

Prados, John, *America Confronts Terrorism*, Ivan R. Dee, 2002.

Prasad, Sakthi, “Microsoft Wins Court Approval to Topple Botnet,” Reuters, 25 February 2010.

Putnam, Tonya, and David Elliott, “International Responses to Cyber Crime,” in Abraham Sofaer and Seymour Goodman, *Transnational Dimension of Cyber Crime and Terrorism,* 2001, pp. 35-66.

Reidenberg, Joel, “States and Internet Enforcement,” *University of Ottawa Law & Technology Journal,* Vol. 1, No. 213, 2004.

Roth, Brad, “State Sovereignty, International Legality, and Moral Disagreement,” Paper Presented at the Panel on “Questioning the Aspiration to Global Justice,” Annual Meeting of the American Political Science Association, September 2, 2005.

Rötzer, Florian, “Fahndung im Internet, *Telepolis News,* 4 October 2001.

Schwarzenegger, Christian, “Sperrverfuegungen gegen Access-Provider,” in Oliver *Arter* and Florian S. *Jörg,* eds*., Internet-Recht und Electronic Commerce Law*, Stämpfli Verlag*, Bern, 2003*

Seedorf, Jan, “Lawful Interception in P2P-Based VoIP Systems,” in Henning Schulzrinne, Radu State and Saverio Niccolini, eds., *Principles, Systems and Applications of IP Telecommunication. Services and Security for Next Generation Networks*, Springer, 2008, pp. 217-235.

Sieber, Ulrich, “Focus: The Threat of Cybercrime,” *Organised Crime Situation Report 2004,* Council of Europe, 2004.

Sieber, Ulrich, and Phillip Brunst, *Cyberterrorism – The Use of the Internet for Terrorist Purposes,* Council of Europe Publications, 2007.

Sieber, Ulrich, and Malaika Nolde, Sperrverfuegungen im Internet, Duncker & Humblot Gmbh , 2008.

Simon, Matthew, and Jill Slay, “Voice over IP: Forensic Computing Implications,” Proceedings of the 4th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 4, 2006.

Singh, Simon, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, Doubleday, 1999.

Sofaer, Abraham, and Seymour Goodman, “Cyber Crime and Security – The Transnational Dimension,” in Abraham Sofaer and Seymour Goodman, eds, *The Transnational Dimension of Cyber Crime and Terrorism*, Hoover Institution Press, 2001.

Standeford, Dugie, “France to Require Internet Service Providers to Filter Infringing Music,” *Intellectual Property Watch*, 27 November 2007**.**

Swale, Richard, *Voice Over IP: Systems and Solutions*, The Institution of Engineering and Technology, 2001.

Tanenbaum, Andrew, *Computer Networks*, 4th ed., Prentice Hall, 2002.

Taylor, David, “Internet Service Providers (ISPs) and Their Responsibility for Content under the New French Legal Regime,” *Computer Law & Security Report,* Vol. 20, Issue 4, 2004, pp. 268-272.

Thomas, Timothy, “Al Qaeda and the Internet: The Danger of ‘Cyberplanning,’” *Parameters,* Vol. 33, No. 1, Spring 2003, pp. 112–23.

United Nations Counter-Terrorism Implementation Task Force (UN CTITF), Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes, 2009.

Ward, Mark, “Campaigners Hit by Decryption Law,” *BBC News*, 20 November 2007.

Weimann, Gabriel, “How Modern Terrorism Uses the Internet,” *The Journal of International Security Affairs*, Spring 2005, No. 8.

Westby, Jody, International Guide to Combating Cybercrime, American Bar Association, 2003.

Zanini, Michele, and Sean Edwards, “The Networking of Terror in the Information Age,” in John Arquilla and David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy*, Rand Publishing, 2001.

Zeller, Jr., Tom, “On the Open Internet, a Web of Dark Alleys,” *The New York Times,* 20 December 2004.

Zwenne, Gerrit-Jan, “Dutch Telecoms Wants to Force Internet Safety Requirements,” *World Data Protection Report*, Issue 09/07, 2009.

Defence Against Terrorism Review
Vol.3, No. 2, Fall 2010, pp. 59-74
Copyright © COE-DAT
ISSN: 1307-9190

Cyberterrorism: in Theory or in Practice?

Anna-Maria TALİHÄRM
Instructor in Cyber Defence Center of Excellence (CCD COE), Estonia

Abstract: *Numerous attempts to define cyberterrorism have not resulted in a commonly accepted interpretation. Cyberterrorism is frequently discussed in media, politics, and security reports but sadly with great inconsistency regarding the meaning of the concept. The wide media coverage often tends to disregard that, according to the majority of authors, not a single clear case of cyberterrorism has actually been observed. Consequently, the term has been used to describe virtually everything from simple hacking to fatal cyberattacks causing serious financial harm and bloodshed. This article gives a concise overview of the status quo of defining cyberterrorism by examining the different aspects of determining the meaning of the term as well as underlining the commonly supported target-oriented approach.*

Keywords: *Cybercrime, Cyberterrorism, Cyberwarfare, Hacktivism*

Introduction

Although there is a great abundance of different definitions of the idea of “terrorism“[1] in numerous documents, until now a universal definition has not been agreed upon. Taking into account the

[1] Mark Burgess, *Terrorism: The Problem of Definition*, Center for Defense Information, August 1, 2003, at http://www.cdi.org/program/document.cfm?documentid=1564 (last visited 1 July 2011).

supplementary definitions devised by historians, political scientists and sociologists,[2] the state of affairs is well put forward by one author, "above the gates of hell is the warning that all that enter should abandon hope. Less dire but the same effect is the warning given to those who try to define terrorism."[3]

The similar, if not more complex, problem of defining a term arises in the diligent attempts to determine the meaning of cyberterrorism since the addition of the prefix "cyber"[4] has only extended the list of possible definitions and interpretations. The lack of a common understanding of the characteristics of cyberterrorism is inhibiting effective dialogue on the subject and has ultimately resulted in overall terminological confusion. The next paragraphs suggest several reasons for this confusion.

For the purposes of this article, "cyberterrorism" is used in the context of the "theoretical" or "target-oriented" approach referring to all politically or socially motivated attacks against computers, networks and information, whether concluded through other computers or physically, while causing injuries or bloodshed, serious damage or fear comparable to a traditional act of terrorism. This approach will be examined in more detail in Section 2.

Media Hype

Cyberterrorism has been featured in international headlines and listed in top security threats for at least a decade now. The media aims for eye-catching stories and is growingly[5] scrutinizing the issues related to cyberterrorism, analyzing case studies, creating dreadful analogies to past tragedies and vividly depicting the potentially catastrophic threats to critical infrastructure. The frequency of cyberterrorism being mentioned in US newspapers has more than doubled since the 9/11 attacks[6] and the term has been used to describe virtually everything from simple hacking to fatal cyberattacks causing serious financial harm, injuries and bloodshed. Not only do the wide media coverage and various security reports tend not to explain the source and background of the stated facts,[7] they also

[2] Alex P. Schmid and Albert J. Jongman, *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, and Literature*, North-Holland, Amsterdam, 1988, pp. 1 - 32.

[3] David Tucker, *Skirmishes at the Edge of Empire*, Praeger, Westport, 1997, p. 51.

[4] In information technology terminology "cyber-" is frequently used as a prefix. It has derived from the word 'cybernetics' to express the general meaning of "through the use of a computer." Miriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*, Routledge, 2007, p. 16.

[5] *See* Maura Conway, "The Media and Cyberterrorism: a Study in the Construction of 'Reality,'" paper presented at the First International Conference on the Information Revolution and the Changing Face of International Relations and Security, Lucerne, Switzerland, 23-25May 2005, available at http://se2.isn.ch/serviceengine/Files/CRN/46731/ieventattachment_file/F6C4C67B-787E-49CD-82DD-102705970C60/en/MConway_Terrorism.pdf (last visited 1 July 2011).

[6] *Id.*, Table 2.1, at 35.

[7] "It is alarming that so many people have accepted the White House's assertions about cyber-security as a key national security problem without demanding further evidence." Evgeny Morozov, "Cyber-Scare: The Exaggerated Fears over Digital Warfare," *Boston Review*, July/August 2009, available at http://bostonreview.net/BR34.4/morozov.php (last visited 1 July 2011).

often overlook the fact that, according to the majority of authors and experts,[8] that so far not a single clear case of cyberterrorism has been observed.

Several studies have indicated that Internet users[9] and companies[10] officially recognize cyberterrorism as a serious threat[11] they need to deal with. Clearly, the considerable media attention and scary predictions provided by numerous security reports play a key great role in shaping such assumptions and "speaking cyber terrorism into existence"[sic].[12] As a rule, journalists, security companies and government authorities underline the perils of cyberterrorism[13] (the reasons for that being popularity, commercial purposes, and mere convenience)[14] whereas scholars attempt to emphasize the contrast between media-hype and empirical reality.[15]

> Particular emphasis needs to be placed upon the processes whereby national security issues communicatively emerge, and the central role of the media in such emergencies, because the political communication/threat image environment shapes both the information available and the ways ordinary people use it in thinking about politics and national security.[16]

[8] "The consensus among security experts is that there has never been a recorded act of cyber terrorism pre- or post- September 11." Giampiero Giacomello, "Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism," *Studies in Conflict and Terrorism, OSCE Strategy for a Comprehensive Approach to Cybersecurity,* pp. 27, 388 (Draft as of March 1, 2010).

[9] *See e.g*. Pew Research Center's Internet&American Life Project, "The Internet and Emergency Preparedness Survey 2003," available at http://www.pewinternet.org/Reports/2003/The-Internet-and-Emergency-Preparedness/Questions-and-Data/Survey-results.aspx?r=1(last visited 1 July 2011).

[10] AFCOM, 2009/2010 AFCOM Data Center Trends Survey Results & Analysis, available at http://www.afcom. com/ images/AFCOM%202009-2010%20Data%20Center%20Trends%20Survey%20Results%20Analysis%20-%20FINAL.pdf (last visited 1 July 2011).

[11] Dorothy Denning estimated in 2007 that the threat of cyberterrorism was not higher than in 2001. *See* Dorothy Denning, "A View of Cyberterrorism Five Years Later," in *Internet Security: Hacking, Counterhacking, and Society*, Kenneth Himma, ed., Jones and Bartlett Publishers, 2007, available at http://faculty.nps.edu/dedennin/ publications/Cyberterror%202006.pdf. On the other hand, the US Congress was recently warned by a growing threat of a crippling attack on telecommunications and other computer networks; FBI director Robert Mueller claims that the cyberterrorism threat is "rapidly expanding." Mark Mazzetti, "Senators Warned of Terror Attack on U.S. by July."*The New York Times*, 2 February 2010, available at http://www.nytimes.com/2010/02/03 /us/politics/03intel.html (last visited 1 July 2011); Vineetha Menon, "FBI: Cyber Terrorism Threat is 'Rapidly Expanding,'" ITP.net, at http://www.itp.net/ 579523-fbi-cyber-terrorism-threat-is-rapidly-expanding (last visited 1 July 2011).

[12] *See* Conway, *supra* note 5, at 44.

[13] *See e.g.***(ISC)2 US Government Advisory Board Executive Writers Bureau,** "Cyberterrorism: A Look into the Future," *Infosecurity*, available at http://www.infosecurity-magazine.com/view/5217/cyberterrorism-a-look-into-the-future/ (last visited 1 July 2011).

[14] "Talk of large-scale retaliation [cyberterrorism] [is] impractical, if not irresponsible, but also understandable if one is trying to attract attention." Morozov, *supra* note 7.

[15] *See* Conway, *supra* note 5.

[16] *Id.*at 44.

Thus, the great gap between the presumed danger and the known cyberterrorist activities triggers most of the debates around cyberterrorism: some[17] believe that a "digital Pearl Harbor" is a realistic scenario while others[18]doubt the seriousness of the threat. Moreover, it has been argued that the overexaggerated threats and extreme scenarios of an imminent threat of cyberterrorism could devalue the term itself as well as shift attention away from other counterterrorist efforts within the cyberdomain.[19]

> Being conditioned to such a degree of generalized panic, any real cyberterrorist attack that does not follow the simulated scenario and produce the anticipated amount of casualties will fall short of being worthy of people's attention and worry.[20]

Terminology Confusion

As has been already discussed, the term "cyberterrorism" is widely used but sadly with great inconsistency regarding the meaning of the concept. The strong interrelation between the characteristics of cyberterrorism and various other cyberoffences, such as hactivism,[21]has rendered drawing a clear line between the types of incidents to be an increasingly challenging task. The "continuing failure"[22] to distinguish different types of cyberincidents often derives from the difficulties in determining the intent and motivation of the attacker as well as fairly evaluating the level of damage caused.[23] Referring to various cyberincidents without full awareness of the opposing

[17] "[Cyberterrorism] isn't so much a threat to national security as a threat to civilization." Jonathan Adams and Fred Guterl, "Bringing Down the Internet," *Newsweek*, Nov. 23, 2003 (quoting Paul Vixie, president of the Internet Software Consortium), available at http://www.newsweek.com/id/60300 (last visited 1 July 2011);Eugene E. Habiger, White Paper, Cyber Secure Institute, 2010, available at http://cybersecureinstitute.org/ docs/whitepapers/Habiger_2_1_10.pdf (last visited 16 March 2010).

[18] *See*Gabriel Weimann, *Cyberterrorism: How Real Is The Threat?,* U.S. Institute of Peace, 2004, available at http://www.usip.org/files/resources/sr119.pdf (last visited 1 July 2011); Joshua Green, "The Myth of Cyberterrorism," *Washington Monthly*, Nov. 2002, available at http://www.washingtonmonthly.com/ features/ 2001/0211.green.html (last visited 1 July 2011).

[19] See Denning, *supra* note 11.

[20] Francois Debrix, "Cyberterror and Media-Induced Fears: The Production of Emergency Culture," *Strategies* Vol.14, No. 1, 2001, p. 156.

[21] Dorothy Denning, Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services U.S. House of Representatives, May 23, 2000, available athttp://www.stealth-iss.com/documents/ pdf/CYBERTERRORISM.pdf (last visited 2 July 2011).

[22] Michael Stohl, "Cyber Terrorism: A Clear and Present Danger, the Sum of All Fears, Breaking Point or Patriot Games?," *Crime, Law and Social Change*, Vol. 46. No. 4-5, 2006, pp. 223-238, available at http:// www. springerlink.com/content/y816117ww6058jp7/ (last visited 2 July 2011).

[23] *See* Section *2 infra.*

meanings of the concept has led to an unfortunate outcome of terminological confusion and the media inadvertently encouraging the belief that any slightly eminent hacking and cyberattack could be an act of cyberterrorism.[24]

Is Cyberterrorism Outdated?

It appears that using the term "cyberterrorism" is outdated and the term itself is too broad to fully reflect all the different aspects of the phenomenon. Similarly to cyberattacks that are growingly politically, socially and religiously motivated, the widely employed term of 'cyberterrorism' has been gaining parallel more specific notions such as "ideological and political extremism"[25] and "cyber-radicalisation."[26] They characterize cyberattacks with certain elements similar to the theoretical concept of cyberterrorism as described in paragraph 2.1 but should not be used as synonyms of the term.

Given that the world has yet to experience a clear case of cyberterrorism, the current definitions and approaches remain on a theoretical level. In practice we face increasingly common cyberattacks that embrace some of the substantial elements of cyberterrorism, such as political motivation or resulting in serious damage and fear, as well as various ways terrorists use the Internet to support and fulfill their purposes.

In order to examine the characteristics of the 'theoretical' cyberterrorism that are more and more encompassed in contemporary cyberattacks, we have to take one step back to review the two prevalent approaches – 'target-oriented' and 'tool-oriented' – in outlining the meaning of cyber terrorism.

Defining Cyberterrorism: Prevalent Approaches

There are a number of different definitions of cyberterrorism offered in thematic literature. Generally speaking, two main approaches can be distinguished. The first identifies as cyberterrorism all politically or socially motivated attacks against computers, networks and information, whether conducted through other computers or physically, when causing injuries, bloodshed or serious damage, or fear (hereafter 'target-oriented cyberterrorism'). The second labels all actions using the

[24] *See e.g*. Serge Krasavin, "What is Cyber-terrorism?,"Computer Crime Research Center, at http://www.crime-research.org/library/Cyber-terrorism.htm (last visited 2 July 2011)(quoting Reuters, "Canadian boy admits cyberterrorism of his family: "Emeryville, Ontario - A 15-year-old Canadian boy has admitted he was responsible for months of notorious high-tech pranks that terrorized his own family, police said Monday.").

[25] *See*Paul Cornish, *Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks*, Directorate General External Policies of the Union, European Parliament, 2009, available at http://www.isis-europe.org/pdf/2009_artrel_247_09-02-epstudy-cyberterrorism.pdf (last visited 2 July 2011).

[26] Steven Emerson,"The Homeland Security Implications of Radicalization ," Testimony before the United States House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, 20 September 2006, available at http://www.investigativeproject.org/documents/testimony/20.pdf (last visited 2 July 2011).

Internet or computers to organize and complete terrorist actions as cyberterrorism (hereafter 'tool-oriented cyberterrorism').

The majority of the authors believe that the target-oriented approach to cyberterrorism, as sharply captured by Dorothy Denning, describes the phenomenon most accurately whereas the tool-oriented approach is mostly seen as merely cyberactivities that support terrorism. The next paragraphs introduce the reasoning behind the two prevalent approaches.

Target-Oriented Cyber Terrorism

One of the first reported incidents that featured activities analogous to what the elements ofwhat cyberterrorism might be took place in 1997 when ethnic Tamil guerrillas were said to have flooded Sri Lankan embassies with thousands of electronic mail messages. The e-mail messages read "[w]e are the Internet Black Tigers and we're doing this to disrupt your communications."[27] The e-mail bombardment of about 800 emails lasted for approximately two weeks and were said to have the desired effect of generating fear in the embassies.[28] The attack has been argued to be the first known attack by terrorists against a country's computer systems, but is still not classified as a clear case of cyberterrorism.

In response to the growing number of politically motivated hacking and cyberattacks,a 1998 report by the Center for Strategic and International Studies entitled "Cybercrime, Cyber Terrorism, Cyberwarfare, Averting an Electronic Waterloo," put forward one of the first commonly referenced definitions for cyberterrorism. The term was defined as:

> Cyber terrorism means premeditated, politicallymotivated attacks by subnational groups or clandestine agents, or individuals against information and computer systems, computer programs, and data that result in violence against non-combatant targets.[29]

A few years later in 2001 Professor Dorothy E. Denning specified the definition for the Center for Strategic and International Studies,describing cyberterrorism as:

> [Cyberterrorism] is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber terrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.[30]

[27] Dorothy Denning, "Activism, Hactivist, and Cyberterrorism" in *Networks and Netwars*, John Arquilla and David Ronfelt, eds, Rand, 2001, p. 269.

[28] *Id.*

[29] Center for Strategic and International Studies, *Cybercrime, Cyberterrorism, Cyberwarfare, Averting an Electronic Waterloo*, CSIS, 1998**.**

[30] Denning, supra *note* 21

Denning's view is the most often-quoted definition of cyberterrorism and most importantly, her interpretation "creates a distinction between a cyberterrorist and a malicious hacker, prankster, identity thief, cyber-bully, or corporate spy based on the political motivation of the attacker. It also differs from hacking, cracking, phishing, spamming, and other forms of computer-related abuse, though cyberterrorists may use these tactics."[31]

Denning underlines the differences between activism, hactivism and cyberterrorism but agrees that the boundaries between them are somewhat fuzzy. According to Denning, hactivists usually have four main 'weapons':

- virtual sit-ins and blockades (hactivists create so much traffic on a selected website that it gets jammed and cannot function properly),
- e-mail attacks (an email server is attacked with thousands of emails and the action, again, interruptingnormal function),
- hacking and computer break-ins (e.g. breaking in a website to change information, defacement), and
- computer viruses and worms.

As a rule, hactivism is all about political protesting using virtual methods and does not seek to cause great financial harm or injure people; therefore it should not be qualified as cyberterrorism.[32] However, hactivism gives us a glimpse of what could be done by cyberterrorists on a bigger scale as terrorists could use any of the abovementioned tactics to accomplish their politically motivatedgoals.

Denning's approach to cyberterrorism is shared by Stohl and Flemming,[33] and partly supported by Professor Gabriel Weimann, who states that cyberterrorism means only "the use of computer network tools to harm or shut down critical national infrastructures (such as energy, transportation, government operations). . . . Cybercrime and cyberterrorism are not coterminous. . . . Terrorists use of computers as a facilitator of their activities, whether for propaganda, recruitment, datamining, communication, or other purposes, is simply not cyberterrorism."[34] Three aspects of Denning's definition of cyberterrorism merit further emphasis: the political and social motivation, serious damage and fear.

Political and Social Motives

Cyberspace has become a popular battlefield for numerous non-state actors performing an increasing

[31] See (ISC)2, *supra* note 13.

[32] See Denning, *supra* note27.

[33] Peter Flemming and Michael Stohl, "Myths and Realities of Cyberterrorism,"in *Countering Terrorism Through International Cooperation,* Alex P. Schmid, ed., ISPAC (International Scientific and Professional Advisory Council of the United Nations Crime Prevention andCriminal Justice Program), Vienna, 2001, pp. 70-105.

[34] Gabriel Weimann, "Cyberterrorism: The Sum of All Fears,"*Studies in Conflict and Terrorism,* Vol. 28, No. 5, March-April 2005, pp. 129-133.

volume of politically motivated cyberattacks. Recent studies[35] show that the number of reports of cyberattacks and network infiltrations that appear to be linked to nation-states and political goals continue to grow and have an augmented impact on international relations. Lithuania in 2008,[36] Radio Free Europe in 2008,[37]and South Korea in 2009[38] are only a few examples.

Probably until now the most well-known, politically motivated cyberattack took place in 2007 in Estonia where the relocation of a Soviet World War II memorial was followed by an unprecedented amount of coordinated cyberattacks. The incident, mainly comprising of massive denial of service attacks (DoS) and distributed denial of service attacks (DDoS), was targeted at Estonian governmental agencies, banks,media channels and private web sites. At the highest moments, the amount of cybertraffic from outside of Estonia targeting governmental institutions was nearly 400 times higher from its normal rate;[39] as a result, several websites and e-services were shut down.

The attacks against Estonia received worldwide attention,leading some experts to label theevent as the first possible model for cyberterrorism in the world.[40] Not surprisingly, the media did not display excessive modesty in interpreting the incident: the attacks were often described as acts of cyberwar[41] or cyberterrorism.[42] Yet, these attacks are generally not considered to be acts of terrorism because they lacked political/social motivation and did not result in bloodshed or serious damage. No doubt that in the context of information security, terrorists may come in several forms such as politically-motivated, anti-government, anti-world trade, and pro-environmental extremists,[43] and hacking be carried out to express patriotic beliefs,[44] but the mere element of political motivation alone should not be enough to earn the label of cyberterrorism.

[35] McAfee Virtual Criminology Report 2009, McAfee, available athttp://img.en25.com/Web/McAfee/VCR_2009_ EN_VIRTUAL_CRIMINOLOGY_RPT_NOREG.pdf (last visted 2 July 2011).

[36] *See, e.g.*,Enerken Tikk, Kadri Kaska, and Liis Vihul, *International Cyber Incidents: Legal Considerations,* NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia 2010, pp. 50-65.

[37] *Id.* at 36-49.

[38] Siobhan Gorman and Evan Ramstad, "Cyber Blitz Hits U.S., Korea," *Wall Street Journal,* 9 July 2009, available at http://online.wsj.com/article/SB124701806176209691.html (last visited 16 March 2010).

[39] Eneken Tikk and Reet Oorn, "Legal and Policy Evaluation: International Coordination of Prosecution of Cyber Terrorism,*"Responses to Cyber Terrorism,* NATO Centre for Excellence – Defence against Terrorism, 2007, p. 96.

[40] Clay Wilson, *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress,* Report for Congress RL32114, Congressional Research Service, 2008, p. CRS-8, available athttp://www.fas.org/sgp/crs/terror/RL32114.pdf (last visited 2 July 2011).

[41] Ian Traynor , "Russia Accused of Unleashing Cyberwar to Disable Estonia," *The Guardian,* 17 May 2007, available at http://www.guardian.co.uk/world/2007/may/17/topstories3.russia (last visited 2 July 2011).

[42] Lain,' "Cyber-Terrorism Has Become a Reality - The Russia-Estonia Cyber-Terrorism Face Off,“ Yahoo, at http://www.associatedcontent.com/article/277054/cyberterrorism_has_become_a_reality.html (last visited 2 July 2011).

[43] Lech Janczewski and Andrew Colarik, *Cyber Warfare and Cyber Terrorism,* IGI Global, 2007, p. xiii.

[44] *See, e.g.* Tikk, *supra* note 36, at 31-32.

The cyberincidents that have so far generated the most damage and fear[45] have not been conducted with the intent to create social and political confusion. Rather, the worst Distributed Denial of Service (DDoS) attacks have been aimed at "extorting money from victims, putting competitors out of business, and satisfy[ing] the egos and curiosity of young hackers."[46] In other words, the political motivation of the attack should not be confused with personal or financial purposes that are more characteristic of cybercrime.

Serious Damage

According to Denning's definition,[47] cyberattacks that would qualify as cyberterrorism should, in addition to having a political or social motivation, bring about a sufficient degree of destruction and disruption in order to generate as much fear and chaos as traditional (physical) acts of terrorism. Attacks against critical infrastructure, such as electrical power, telecommunications, water supply, oil and gas, and financial institutions, that result in serious damage could be considered to be cyberterrorism. On the other hand, cyberattacks that are launched against banks and stock exchanges and result in millions of dollars of damage but do not include the element of social and political motivation should not be labeled cyberterrorism.

Until now, one of the most severe attacks reported against critical infrastructure involved an Australian man penetrating the local waste management system and using radio transmissions to alter pump station operations.[48] Even though spilling a million liters of raw sewage caused serious damage, this act cannot be considered to be cyberterrorism just because the Internet provided the means of the attack because the man did not act with the goal to coerce the 'statist' society.

However, serious impact should not always imply critical financial consequences but can also constitute a grave violation of "human rights," such as freedom of information, access to public services or informational privacy – rights that are increasingly self-evident to societies with a high level of IT infrastructure. Thus, the identification of a possible case of cyberterrorism depends on the various viewpoints of 'serious damage' that need not be solely measurable in traditional monetary terms.

[45] *See e.g.* EllenNakashima, "More than 75,000 Computer Systems Hacked in One of Largest Cyber Attacks, Security Firm Says,"*The Washington Post,* 18 February 2010, available at http://www.washingtonpost.com/wp-dyn/content/article/2010/02/17/AR2010021705816.html (last visited 2 July 2011).

[46] Denning, supra *note* 11, at 2.

[47] *See* Denning, supra note 30 and associated text.

[48] Michael Crawford, "Utility Hack Led to Security Overhaul," *Computerworld,* 16 February 2006, available at http://www. computerworld.com/s/article/108735/Utility_hack_led_to_security_overhaul (last visited 2 July 2011).

Similar arguments regarding damage that cannot be measured solely in terms of numbers is brought up by Susan Brenner,[49] who explains that 'damage' in the context of terrorism involves the intention to demoralize the population either directly or indirectly.[50] So far the motivation of terrorists has primarily and 'directly' constituted in "demonstrating citizens' vulnerability"[51] by destroying property and causing injuries or bloodshed. Brenner argues that cyberterrorism aims to achieve the same goals as terrorism but in an indirect manner by "using technology to erode our confidence in the information and the systems we necessarily rely on to function in our modern, urban environments."[52]

Fear

Fear comparable to a traditional act of terrorism is another characteristic of a politically motivated cyberattack that fits into the theoretical concept of cyberterrorism. By combining the aspects of political and social motivation withthat of serious damage and fear, Rollins and Wilson have described a two-fold definition of cyberterrorism:

- Effects-based: cyberterrorism exists when computer attacks result in effects that are disruptive enough to generate fear comparable to a traditional act of terrorism, even if done by criminals.
- Intent-based: cyberterrorism exists when unlawful or politically motivated computer attacks are done to intimidate or coerce a government or people to further a political objective, or to cause grave harm or severe economic damage.[53]

This isa simplified approach; it is interesting to observe that the first of the two classifications seems not to require political or social motivation but instead highlights the aspect of causing fear comparable to a traditional act of terrorism.

The element of fear in cyberterrorism should be considered from two angles. On one hand, fear and confusion can be the result of the mere use of the term 'cyberterrorism' in its present inconsistent manner. Embar-Seddon argues that:

> The most destructive forces working against an understanding of the threat of cyberterrorism are a fear of the unknown and a lack of information or, worse, too much misinformation. The word cyberterrorism brings together two significant

[49] Brenner distinguishes three categories on how terrorists can use computer technology to fulfill their goals, by using computer technology as a: weapon of mass destruction, weapon of mass distraction, or weapon of mass disruption. See Susan Brenner, *Cyberthreats: The Emerging Fault Lines of the Nation State, Oxford University* Press, 2009, pp. 44-54.

[50] John Rollins and Clay Wilson, *Terrorist Capabilities for Cyberattack: Overview and Policy Issues,* Report for Congress RL33123, Congressional Research Service, 2007, available at http://www.fas.org/sgp/crs/terror/ RL33123.pdf (last visited 2 July 2011).

[51] Brenner, supra note 49, at 41.

[52] *Id.* at 42.

[53] Wilson and Rollins, supra note 50, at CRS-3.

> modern fears: the fear of technology and the fear of terrorism. Both technology and terrorism are significant unknowns.[54]

Thomas adds "[t]he Internet produces an atmosphere of virtual fear or virtual life. People are afraid of things that are invisible and things they don't understand. The virtual threat of computer attacks appears to be one of those things."[55]

On the other hand, large-scale cyberattacks have the potential to bring along significant chaos and loss of control over our everyday lives that are increasingly dependent on information technology. Citizens of modern information societies may already, or shortly begin to, value attacks against their 'virtual well-being' on the same scale as attacks against their physical health and wellness. Some believe that in a way such fear can be "as demoralizing as the 9/11 attacks."[56]

Either way, creating fear, chaos and confusion is one of the goals of cyberterrorism. Fear has the psychological effect of making citizens act in certain ways (e.g. agree to bigger expenses in national security or buy more Information Technology (IT) security products[57]) and therefore more easily manipulated. Additionally, fear of cyberterrorism makes communities more observant about security threats and may in the long run create a better level of information security.However as correctly concluded by Stohl: "We must remember that generating an unwarranted fear of potential attack, even while preparing to defend against it, serves the cause of the terrorist even if the security precautions are ultimately successful."[58]

Tool-Oriented Cyber Terrorism

Although authors and experts commonly support the target-oriented approach, several other sources such as media, security reports, and politicians estimate that cyberterrorism additionally includes various activities how terrorists use the Internet to pursue their terrorist goals. The list includes such Internet-based actions as propaganda via terrorist websites, public relations, providing information such as sharing instructions and detailed manuals,[59] data mining, fundraising and

[54] Ayn Embar-Seddon, "Cyberterrorism: Are We Under Siege?"*American Behavioral Scientist,* Vol. 45, No. 6, February 2002, pp. 1033–1043.

[55] Timothy L. Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning,'"*Parameters*, Vol. 33, No. 1, Spring 2003, pp. 112–23, available athttp://www.iwar.org.uk/cyberterror/resources/cyberplanning/al-qaeda.htm (last visited 2 July 2011).

[56] Brenner, supra *note* 49.

[57] See e.g. Stohl, supra note 22.

[58] *Id.*

[59] Gabriel Weimann, *WWW.TERROR.NET: How Modern Terrorism Uses the Internet,*U.S. Institute for Peace, Washington DC, 2004, available at http://www.usip.org/pubs/specialreports/sr116.pdf (last visited 2 July 2011).

financing,[60] internal networking and international connections,[61] communications, and recruitment.[62]

These activities do not directly result in great financial loss or harming peoples' lives, but it is nevertheless argued that by adopting a wider notion of cyberterrorism, one can focus on the "full range of legal concerns and responses."[63] The same approach suggests[64] that Denning's definition depicts 'pure cyberterrorism' and is too narrow of a term. For example, Gordon and Ford label all supporting activities of terrorism carried out via Internet or computers "the new terrorism" and stress that the real danger lies in not seeing the "big picture" of the overall terrorist threat.[65]

Such online activities, as listed above, may extensively facilitate reaching terrorists' goals as well as supporting fulfilling their missions and must therefore be scrutinized, countered and prevented. However, these activities should be considered as supporting actions of cyberterrorism and for the sake or terminological clarity not be included in the theoretical concept as described in Section 2.1.

Conclusion

Cyberattacks are an increasingly common nuisance but so far they have not been conducted by terrorists seeking to inflict the kind of damage that would qualify them as cyberterrorism by most definitions. Despite the claims that cyberterrorism might be the fruit of a successful media hype and overexaggeration, the idea has stayed on the public agenda for decades now.

The terminology confusion accompanying the debates over cyberterrorism raises the question whether it is feasible or overall possible to clearly define an incident that has never taken place. The answer to that would certainly not change the threat or the fear of a possible large-scale cyberattack. Most likely, as long as there is no common definition of 'terrorism' and various institutions perform on the basis of their own differing operational definitions, there will be no interest to limit the meaning of the term and'cyberterrorism' will not be bound to a universal definition as well.

[60] Wilson and Rollins, supra *note* 50, at CRS-20.

[61] John Arquilla, David Ronfeldt, and Michele Zanin, "Networks, Netwar and Information-Age Terrorism," in *Countering the New Terrorism,* Ian O. Lesser, et al, eds, Rand, 1999, available athttp://www.rand.org/publications/MR/MR989/MR989.chap3.pdf(last visited 2 July 2011); Arquilla and Ronfeldt, supra note 27.

[62] See,e.g.,Maura Conway, "Terrorist 'Use' of the Internet and Fighting Back,"paper prepared for presentation at the conference Cybersafety: Safety and Security in a Networked World: Balancing Cyber-Rights and Responsibilities, Oxford Internet Institute (OII), Oxford University, UK, 8-10 September, 2005, available athttp://www.oii.ox.ac.uk/microsites/cybersafety/extensions/pdfs/papers/maura_conway.pdf (last visited 2 July 2011); Phillip Brunst, Use of Internet by Terrorists – a Threat Analyses, in Responses to Cyber Terrorism. NATO Centre of Excellence – Defence Against Terrorism, 2008, pp. 34-60.

[63] Clive Walker, "Cyber-Terrorism: Legal Principle and Law in the United Kingdom,*"Pennsylvania State Law Review,* Vol. 110, No. 3, 2006, p. 634, available athttp://www.court21.ac.uk/docs/penn07d.pdf (last visited 2 July 2011).

[64] *See* Sarah Gordon and Richard Ford, *Cyberterrorism?,* Symantec White Paper, 2003, available at http://www.symantec.com/avcenter/reference/cyberterrorism.pdf(last visited 2 July 2011).

[65] *See* Id.

This article argues that there is a gap between the theoretical definition of cyberterrorism and the terrorist use of the Internet we are facing today. While the target-oriented approach refers to “all politically or socially motivated attacks against computers, networks and information, whether concluded through other computers or physically, by causing injuries or bloodshed, serious damage or fear comparable to a traditional act of terrorism,” and thereby outlines a solid set of characteristics of the concept of cyberterrorism, in practice, the term is rarely used with this meaning. Hence, decades of careful deliberation and the relatively high popularity of the issue have unfortunately led to a kind of ‘dead end’ where cyber terrorism means everything and nothing at the same time.

Surely, the lack of a unified approach to the key elements of cyberterrorism will not diminish the significance of being prepared for a possible politically and socially motivated cyberattack that could bring about serious damage and fear. But as previously argued by Stohl, creating panic and fear about possible terrorist cyberattack will eventually not work to the benefit of the population but support the terrorists’ goals to intimidate the people and the government.

Using the term ‘cyberterrorism’ to describe a particular cyber incident should be put avoided until the facts of the case can be matched with the combination of political or social motivation, serious damage, and fear. Still, we should continue to be vigilant about the increasing frequency and sophistication of politically motivated cyberattacks, hactivism, patriot hacking and the terrorist use of the Internet as it will reflect the level of the threat and the capability of terrorists to launch an attack of target-oriented cyberterrorism.

References

Adams, Jonathan, and Fred Guterl, "Bringing Down the Internet," *Newsweek*, Nov. 23, 2003.

Brenner, Susan, *Cyberthreats: The Emerging Fault Lines of the Nation State*, Oxford University Press, 2009.

Burgess, Mark, *Terrorism: The Problem of Definition*, Center for Defense Information, August 1, 2003.

Cavelty, Miriam Dunn, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*, Routledge, 2007.

Center for Strategic and International Studies, *Cybercrime, Cyberterrorism, Cyberwarfare, Averting an Electronic Waterloo*, CSIS, 1998**.**

Conway, Maura, "The Media and Cyberterrorism: a Study in the Construction of 'Reality,'" paper presented at the First International Conference on the Information Revolution and the Changing Face of International Relations and Security, Lucerne, Switzerland, 23-25May 2005.

Cornish, Paul, *Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks*, Directorate General External Policies of the Union, European Parliament, 2009.

Crawford, Michael, "Utility Hack Led to Security Overhaul," *Computerworld,* 16 February 2006.

Debrix, Francois, "Cyberterror and Media-Induced Fears: The Production of Emergency Culture," *Strategies* Vol.14, No. 1, 2001.

Denning, Dorothy, Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services U.S. House of Representatives, May 23, 2000.

Denning, Dorothy, "Activism, Hactivist, and Cyberterrorism" in *Networks and Netwars,* John Arquilla and David Ronfelt, eds, Rand, 2001.

Denning, Dorothy "A View of Cyberterrorism Five Years Later," in *Internet Security: Hacking, Counterhacking, and Society*, Kenneth Himma, ed., Jones and Bartlett Publishers, 2007.

Embar-Seddon, Ayn "Cyberterrorism: Are We Under Siege?" *American Behavioral Scientist,* Vol. 45, No. 6, February 2002, pp. 1033–1043.

Emerson, Steven, "The Homeland Security Implications of Radicalization ," before the United States House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, 20 September 2006,.

Flemming, Peter, and Michael Stohl, "Myths and Realities of Cyberterrorism," in*Countering Terrorism Through International Cooperation,* Alex P. Schmid, ed., ISPAC (International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice Program), Vienna, 2001, pp. 70-105.

Giacomello, Giampiero, "Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism," *Studies in Conflict and Terrorism*, *OSCE Strategy for a Comprehensive Approach to Cybersecurity,* pp. 27, 388 (Draft as of March 1, 2010).

Gorman, Siobhan, and Evan Ramstad, "Cyber Blitz Hits U.S., Korea," *Wall Street Journal*, 9 July 2009, available at http://online.wsj.com/article/SB124701806176209691.html (last visited 16.03.2010).

Green, Joshua, "The Myth of Cyberterrorism," *Washington Monthly*, Nov. 2002.

Habiger, Eugene E., White Paper, Cyber Secure Institute, 2010.

Janczewski, Lech and Andrew Colarik, *Cyber Warfare and Cyber Terrorism*, IGI Global, 2007.

Mazzetti, Mark, "Senators Warned of Terror Attack on U.S. by July."*The New York Times,* 2 February 2010.

Morozov, Evgeny, "Cyber-Scare: The Exaggerated Fears over Digital Warfare," *Boston Review*, July/August 2009.

Nakashima, Ellen, "More than 75,000 Computer Systems Hacked in One of Largest Cyber Attacks, Security Firm Says," *The Washington Post,* 18 February 2010.

Rollins John, and Clay Wilson, *Terrorist Capabilities for Cyberattack: Overview and Policy Issues,* Report for Congress RL33123, Congressional Research Service, 2007.

Schmid, Alex P., and Albert J. Jongman, *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, and Literature*, North-Holland, Amsterdam, 1988.

Stohl, Michael, "Cyber Terrorism: A Clear and Present Danger, the Sum of All Fears, Breaking Point or Patriot Games?," *Crime, Law and Social Change*, (46)4-5, 2006, pp. 223-238.

Tikk, Enerken and Reet Oorn, "Legal and Policy Evaluation: International Coordination of Prosecution of Cyber Terrorism," *Responses to Cyber Terrorism*, NATO Centre for Excellence – Defence against Terrorism, 2007, p. 96.

Tikk, Enerken, Kadri Kaska, and Liis Vihul, *International Cyber Incidents: Legal Considerations,*NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia 2010, pp. 50 - 65.

Tucker, David, *Skirmishes at the Edge of Empire*, Praeger, Westport, 1997.

Weimann, Gabriel, *Cyberterrorism: How Real Is The Threat?,* U.S. Institute of Peace, 2004.

Weimann, Gabriel, "Cyberterrorism: The Sum of All Fears," *Studies in Conflict and Terrorism*, Vol. 28, No. 5, March-April 2005, pp. 129-133.

Wilson, Clay, *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress,* Report for Congress RL32114, Congressional Research Service, 2008.

.

Defence Against Terrorism Review
Vol.3,No.2,Fall 2010,pp.75- 85
Copyright © COE-DAT
ISSN: 1307-9190

Radicalization on the Internet

Julian CHARVAT
Former Course Director in COE-DAT, Major in U.K Armed Forces

Abstract: *This paper discusses the process of radicalization. It will look at how and why some people are vulnerable in society and targeted by terrorist organizations in an attempt to recruit them. It will also consider some of the individual reasons that a person is moved to carry our criminal acts and cause mass casualties. It will further consider the possible approach needed to avoid radicalization and attempt to reduce terrorist recruitment.*

Keywords: *Terrorism, Radicalization, Recruitment, Psychology*

Introduction

The debate continues within both academic and security circles as to the exact nature of 'cyberterrorism.' As with terrorism itself, there is no clear and universally agreed upon definition of 'cyberterrorism.' Using narrow definitions,[1] it can be argued that there has never been a cyberterrorist

[1] "Attack on information systems by a known terrorist group for the primary purpose of creating alarm and panic" or "An attack suing information systems to threaten/destroy property or lives."

attack as the known attacks in cyberspace to date do not meet the traditional definition of terrorism.[2] On the other hand, using wider definitions,[3] it can be argued that every terrorist use of cyberspace is 'cyberterrorism' and it is happening constantly. There are of course many views covering the entire spectrum in between. This is the subject of a paper in its own right. Leaving the debate on definitions aside, this paper aims to discuss use of the Internet by terrorist groups as a radicalization and recruiting tool.

Terrorism needs terrorists. As simple as this might sound, a terrorist organization can only survive if it has enough active members who are radicalized and committed to the extent that they will commit acts of violence for their cause. The issue of radicalization is one that affects all terrorist groups. It is not just a religious issue but also the process that draws someone from being a passive supporter of a view to being an active foot soldier as a terrorist. The process can be gradual or instant and will be impacted by the life experience of the individual.

Well, what is radicalization? In the context of looking at modern terrorist organizations, it is the galvanization of people to an extreme[4] religious or political view. Given the nature of terrorism as a politically motivated action and that only the most committed followers of a cause will commit such acts as to kill and maim unknown people, the fight against radicalization, whatever the belief of the people being radicalized, is a key activity in defeating terrorism.

There are many terms being used in modern parlance regarding terrorism. These can become confusing and dangerous, especially when dealing with a religio-politically motivated terrorist organization such as al-Qaeda. Fundamentalism and radical religion are different things, although there may be some areas of overlap in the two. For the purpose of clarification, this paper will refer to radicals and by that it is meant as those who purport such an extreme view or belief that they will use indiscriminate lethal violence to express it. Radicalization is a process that indoctrinates someone to a certain belief or point of view far beyond the accepted mainstream interpretation or understanding of it and will alter their behavioral boundaries considerably.

Strata of Support

Most people will be in a group that can be classed as the General Population. These are citizens who lead a normal and lawful life and want to live in a way that does not impinge on others. This group encompasses all backgrounds, economics, races and religions who lead a peaceful life and undertake

[2] For example, the US Department of State defines terrorism as "premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents."

[3] "The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm of further social, ideological, religious, political or similar objectives." B. Collin, Institute for Security and Intelligence.

[4] Cultural context is everything in deciding the 'norm.' In different countries at different times there were many different definitions of "extremism." For example, the UK Government defines 'violent extremism' as: "The demonstration of unacceptable behaviour by using any means or medium to express views which foment, justify or glorify terrorist violence in furtherance of particular beliefs; seek to provoke others to terrorist acts; foment other serious criminal activity or seek to provoke others to serious criminal acts; or foster hatred which might lead to inter-community violence in the UK."

in democratic principles and the rule of law. They will completely condemn terrorism as wrong even if they share the political views, ethnicity or religion of the terrorist organization. The General Population believes in the ballot box and legitimate political action, including lawful protest and demonstration as the only way of making their voice heard when they wish to influence government or society and would accept consensus even if they disagree with the outcome. Basically anyone not inclined towards the terrorist cause or action is classed in this group for the purpose of this model.

Sympathizers are at the very start of the radicalization process and would be considered as being vulnerable to arguments which would change their viewpoint *vis-a-vis* the beliefs and viewpoints of a terrorist organization. This group is made up of people who would condemn terrorism completely even though they feel a kinship with the terrorist's aims if not with their action. While they would not knowingly support terrorism, they might campaign or be active in legitimate political action or protest in favor of the same cause as the terrorist organization. They oppose the violence but may be involved in a front organization in their legitimate political campaigning. An example of this might be an animal lover. This could be someone who shares the same end view as a single-issue terrorist in ending cruel farming practice or unnecessary experimentation on animals. Like the terrorist, they want a change in government policy. However, they would only consider lawful action, legitimate protest and customer choice as their weapons. They would not only condemn the terrorist but would take full and active steps to report any terrorist action or suspicion to the law enforcement agencies in order to prevent a terrorist act being carried out. They would regard the violence of terrorism as a greater threat than the cause they oppose.

Supporters are people who are of the same view as the terrorists and while they personally participate in only legitimate lawful political campaigning and activities, they feel that they can understand the need for violence and do not completely condemn the terrorists. These people will campaign for the issue for which the terrorists act and will justify, at least to some extent, the need for terrorism. Supporters will campaign in lawful protests but often try and provoke a reaction from the security forces. They would not actively encourage or assist in a terrorist attack itself but are less likely to inform the authorities if they had information about terrorist activity and may not hamper terrorist activity. These people are highly vulnerable to further radicalization and terrorist recruitment; they would be actively sought by a terrorist groomer if they expressed their views in a chat room, for instance.

Activists are those who are fully supportive of terrorism but have not yet committed terrorist acts. They will publicly support terrorist causes, attend rallies, write articles and distribute leaflets in support of the terrorist cause. They are likely to raise funds and profile of the terrorists, but will generally be outside the terrorist organization's decisionmaking and actiontaking circles. They may be involved in logistics or even provide assistance such as safe houses and are vital to the terrorist organization as they can operate in the 'normal' world. This group will include potential future terrorists who are being groomed and readied, who may at some point cross that line into becoming fully fledged terrorists by committing actual terrorist acts.[5]

[5] Marc Sageman, "Leaderless Jihad, Terror Networks in the 21st Century," University of Pennsylvania Press (2008). Sageman discuss the Internet and its relationship with the radicalization process in detail in Chapters 4 and 6.

Terrorists are those who have been radicalized into taking direct action and actually commit or assist in the commission of terrorist acts. These are people who have a combination of extreme views and life circumstances that have combined to radicalize them to such an extent that the will risk imprisonment or their own lives in order to further the cause that they have been radicalized to support.

Radicalization Process

Terrorists have become adept in using the Internet as an important tool in the radicalization process. This can be through a wide and growing number of methods, including straightforward propaganda, misinformation about the target government, grooming or misinforming young people in chat rooms and forum sites, and developing interactive games to demonize their 'enemy.' Radicalization can occur for any cause or reason. Terrorists will look for people whom they regard as vulnerable and try to suggest or enhance views held by an individual and push them along a path of radicalization towards terrorism. There are of course many life experiences that individuals have that can push along that path. These will vary and are ultimately unique in each case.

It is necessary to understand the individual factors and experiences that draw people into terrorism which collectively form an important part of the radicalization process. Without willing foot soldiers to carry out the acts themselves, there would be no terrorist action despite groups existing who are motivated to support terrorist activity. There will always be those who sympathize or even support the terrorist activity and have the same motivations as the terrorist organization but stop short of conducting a terrorist attack. If we look at what draws an individual to cross the line to become an active terrorist, we may be able to spot the danger signs and prevent or dissuade that person from such a course of action before they become sufficiently radicalized to commit a terrorist act.

There are many risks and dangers associated with being a terrorist, whatever the motivation and role. It is worth examining why people become terrorist foot soldiers to understand how to prevent the process of radicalization from getting that far. There has been much debate about the mental state of a terrorist. What would drive a person to deliberately kill or maim their fellow man in great numbers? There had been arguments that they must be psychopathic or mentally feeble and have been exploited and encouraged into terrorism by those who want to keep their hands clean. Research is limited as terrorists are difficult to find for psychoanalysis; however study has shown that the 'outstanding common characteristic of terrorists is their normality.'[6] There may be many factors that drive an otherwise normal individual to such abnormal extremes.

A terrorist group may be appealing to certain types of people who share the same views but seek something in their lives that membership in such an organization can provide. It may fulfill a sense of belonging to a group or personal worth. In some societies, terrorist activists are given high social regard and this will encourage certain types of people to become a terrorist. As Martha Crenshaw observed:

> The incentives for joining a terrorist organization, especially one that is already established and of known character, include a variety of individual needs: to belong to

[6] Crenshaw, The Causes of terrorism.

> a group, to acquire social status and reputation, to find comradeship or excitement, or gain material benefits. The popular image of the terrorist as an individual motivated exclusively by a deep and intransigent political commitment obscures a more complex reality.[7]

The personality of an individual is obviously a factor in their initially becoming a terrorist activist and the subsequent transition from activist to fully fledged terrorist. They must also share the beliefs or agree with the propaganda of the terrorist organizations. Social, political and economic factors will likewise be important in profiling vulnerable people who may move on from being a law-abiding member of the public to become a terrorist activist and then a potential terrorist for the future.

While sympathy for the motivation of a terrorist organization and certain personality traits may make one person more likely to become a terrorist activist than another, there is usually a final factor that will push them to activism. Poverty is often thought to be a major factor in driving people into terrorism. While undoubtedly some terrorists come from poverty, it is not in itself the sole factor in driving someone to terrorism. Indeed Paul Wilkinson has argued that poverty or deprivation does not automatically result in aggression and violence.[8] He proposes that the poorest masses of the Third World are not prepared for revolutionary struggles or even political participation because they are completely engrossed in the struggle to stay alive. In fact Alberto Abadie believes that terrorists are more likely to spring from developing societies rather than rich or poor ones.[9] Terrorists do exploit poor people and some acts of terrorism have been carried out for financial gain. This, however, is not poverty causing terrorism, but in the cases of poor people being exploited to plant a bomb, the attack would still be planned and executed without the poor people doing it, because the organization would use and recruit a committed terrorist instead. There would still be terrorism without poverty. Educational opportunities have likewise been examined as a possible cause for people resorting to practice terrorism. It was considered if terrorists were more likely to be ill-educated and act out of ignorance or simplicity. This was found not to hold water as more terrorists were found to be educated to a reasonable standard. Generally the leaders of a terrorist group will be well educated and the longevity of the group may be dependent on its leader's intelligence and education level. In many ways a terrorist organization is like any other type of organization – it needs people from all levels of education and intelligence to employ them for tasks appropriate for their abilities.

Social inequality and humiliation are two of the major reasons cited by terrorists in explaining their rationale for committing acts of terrorism.[10] The poorest societies in the world work hard for survival and generally accept their circumstances. However, societies where there is a large

[7] Crenshaw, Theories of terrorism

[8] Paul Wilkinson is a former director of St Andrew's University CSTPV. This quote comes from the St. Andrew's University CSTPV Certificate in Terrorism Studies, Course Notes – Module A, Lesson 4, "Cultural, Economic and Other Factors."

[9] Alberto Abadie is a Professor of Public Policy at Harvard University. Alberto Abadie, "Poverty, Political Freedom and the Roots of Terrorism," National Bureau of Economic Research Working Papers, 2004.

[10] St Andrew's University CSTPV Certificate in Terrorism Studies Course Notes – Module A, Lesson 4, 'Cultural, Economic and Other Factors'.

economic or social inequality often have a greater problem. This is because there are disaffected people who feel unfairly treated. While the vast majority of people will address this by working to change their opportunities or circumstances through hard work or legitimate political protest, there are some who will be more likely to be attracted to terror. Yigal Cameron noted this at the 2005 Madrid Summit:

> Economic change creates conditions that are conductive for instability, the emergence of militant movements and extremist ideologies. In the Islamic world, for example, the more traditional segments of the population are disorientated by sweeping socio-economic change, and are therefore especially susceptible to movements that strengthen threatened identities provide explanations, and gives believers a sense of empowerment.[11]

Perceived humiliation is generally accepted as a major factor for those who become terrorists in making that decision. They feel that they personally, their family or their culture have suffered a humiliating action from the target population or government. This could be a historical event where the terrorist's people suffered a defeat or occupation. This is hard to counter as it will be hatred and distrust that have been integral to the upbringing of the person and be part of their make-up. This could also be a more recent event where security forces have overreacted and handled a situation poorly – thus pushing a sympathizer into full blown terrorism. An example of this was the British Stop and Search policy in Northern Ireland in the early 1970s. While a militarily useful tool in finding illegal weapons, the searches were poorly planned and often clumsy while becoming a focus of resentment for young Catholic men in Northern Ireland as they were the primary target for the searchers. It could also be borne from the current situation. Al Qaeda often portrays the fact infidel troops are on holy Arab lands as a humiliation and therefore encourages some to take up action. Jessica Stern noted:

> I've been interviewing terrorists around the world for these past 5 years [written in 2003]. Those I interviewed cite many reasons for choosing a life of holy war……. the variable that comes up the most frequently is not poverty or human-rights abuses, but perceived humiliation.[12]

Propaganda and Message

Radicalization can be a complex process. The Internet has given people a new and unregulated medium for advice and information. By the very nature of the Internet, people can pose as who they want to be and not necessarily who they are. People will try and find answers to questions on the Internet, and unlike a book where most people will (or at least could) check the author and publisher for credibility, people often take information posted on the Internet at face value. While published books can contain any point of view, there is a publisher who has to be identified and who is presumably subject to the law. Publishers also have reputations and will guard these; books that have obviously wrong information are unlikely to be put on the shelves by a 'serious' publisher. The

[11] The Madrid Summit Working Paper Series

[12] Stern, Terrorism's new Mecca

Internet is unregulated and it is not possible to immediately know the quality of a website. It is the skill of the webmaster that will determine how professional a website looks, not the content of the articles. Finding a book by a renowned author published by a known house is a guarantee that it is a genuine book. A website may not have any input from the people it claims as contributors.

Many young people use the Internet to answer questions they have about life in general or specific areas they are interested in and find people happy to answer. While the majority of these sites have honest people helping out others, some will be either established by or be patrolled by terrorists looking for the vulnerable who are asking questions they can capitalize on. Terrorist can put up their own messages with spurious proof to back up what they say. A youngster is unlikely to do a lot of fact-checking and with patience the terrorist group may be able to manipulate the youngster's way of thinking. Terrorists can draw on actions or statements by the governments or organizations that they intend to target. They will also use the Internet to justify and glorify their actions. The terrorists will provide a slanted perception and attempt to make themselves legitimate to corrupt the minds of those they are engaging.

Terrorists use the Internet for many reasons. As, by its very nature, terrorism has a message, the Internet provides an opportunity for them to get that message out, both to the world at large and, more importantly, to those who they may be able to actively sway to their cause. This is important in the radicalization process as those who are vulnerable to recruitment are likely to search for and visit these sites. Unlike official web pages, terrorists are not bound by truth or honesty and will give slanted messages to promote their causes. The Internet provides many advantages for the terrorist. These allow them to find and entice the vulnerable, especially the young, to believe or support them. And they can do this at little or no cost, from anywhere in the world, and often with little chance of being caught.

Terrorists are generally good at propaganda and as they are not bound by the truth or reality as we are, they have a great scope to exploit the use of the Internet for this purpose. Terrorists have a message, which comes from their motivation, which they want to share with the world. Terrorists are not mad people and, in their own view, are not even bad people; therefore they believe they can explain their cause or educate people to their perceived problem or grievance. Video sharing is a popular way for them to do this. They may show the actions of their own people edited to stirring music to glorify the action to gain support from those likely to agree with them. The may choose to show pictures of those allegedly killed by the security forces or other material which may support their cause. A prime example of this is Terrorist (Irhabi) 007, or Younis Tsouil. He was an active hub for processing and posting terrorist material on the Internet which had incited terrorist activity and murder. An associate who has committed over € 2.5M of fraud to fund cyber campaigns funded this activity. Developing sites that masquerade as legitimate news and media sites are of extreme interest to the terrorist organization. There have been several examples of such sites being set up or exploited for terrorist purposes. *An Phoblacht*, the Sinn Fein weekly newspaper, clearly supported the IRA terrorists during the Northern Ireland troubles and was the first Irish paper to provide an online version. This website still provides a strong Republican message. Such websites are often distanced from the terrorists themselves to give an air of legitimacy but are a clear tool in supporting them.

Forum and Chat Rooms

Recruitment is one area which has benefited tremendously from the advent of the Internet. Using the technology of the Internet, people communicate with each other instantly and anonymously on line. They can ask questions on forum sites as well as engage in real-time conversations in chat rooms. Terrorist groups will have links to these from their own websites in order to get potential supporters. They will often participate in chat rooms to find out who might be susceptible to the terrorist message. Those assigned to monitor chat rooms will do this and then pass information on selected people onto a middleman who will confirm their commitment in greater detail. The middleman will then pass selected individuals on to the first actual terrorist contact who may arrange a meeting to begin the physical and mental preparation. Obviously terrorists had been successfully recruited for thousands of years before there was an Internet, but cyberspace has given them a wider net and more chance for disaffected individuals to find the terrorist recruiter. It also presents an opportunity for defence against terrorism. If such sites and chat rooms are found, then the security forces may be able to intervene or even launch a countercyber campaign to deradicalize those who the terrorists are trying to radicalize. This of course is dependent on national laws and policies. In countries where there is some guarantee of free speech, it is often more difficult for the authorities to shut down a site, no matter how hateful its message is, unless it can be directly connected to a group that the nation considers to be unlawful. Terrorists groups often use this as a factor in determining where to base their web presence.

Chat rooms are virtual venues where some people go to exchange ideas and answer questions about life. While people mostly use them legitimately, there is a great opportunity to exploit them. Most chat rooms and forum sites are profile-based. Some people will create a profile that is completely spurious and not the person they are pretending to be. The author has monitored some chat rooms and while most talk is benign rubbish, you do get people seeking serious answers. In one room where everyone was anonymous, there was a lot of chat about religion and its interpretation. One guest kept asking to speak to a cleric to answer a serious religious question – several people responded saying they were clerics. Clearly they were not – their other posts were not compatible with those of a cleric! A terrorist groomer would wait and look for such posts and begin engaging the vulnerable mind to the terrorist cause. Forums have the same problems as chat rooms – you only know what the other person says about themselves and not if it is true. Anyone can pose as an expert to post false information. Often other posters will counter but terrorists will have one person take more than one identity at the same time so as to support or vouch for the argument. After gaining interest from an individual, the groomer will then usually seek one-to-one contact. They will often groom chatters to differentiate between someone who is just a curious but innocent youth and someone who has that little more that could single them out as susceptible to radicalization and recruitment.

Terrorists lie – they are not bound by the truth as official agencies are – so it means they can have more engaging and fantastic websites. They will use film, games and ‘serious-looking’ pages to promulgate their message or edit film of their target to make it look as if an event happened differently than reality. Officials often fail to grasp this. There are vulnerable people who genuinely do not know who to believe, the official or the terrorist. Most officials are 'Digital Immigrants' while most terrorists use 'Digital Natives' – and the difference is plain.[13]

An example of this in its early stage was monitored on a mainstream Muslim youth website in the United Kingdom. Hussein was a 15-year-old schoolboy who posted a school project for comment from other members of the forum site. In his post he expressed mixed feelings and uncertainty about how the West saw Islam and the true nature of the Jihad. Hussein stated that he believed Jihad was a personal struggle and it was against Islam to kill. He also expressed that he felt as though the West regarded him as a terrorist because he was Muslim and that there was significant anti-Muslim sentiment in Western society. The first two replies agreed with Hussein that in Islam it is forbidden to kill innocents. 'OBL4Caliph' entered the debate and began saying that he was an authority on Islam and that Jihad was a duty for all Muslims and that it was a requirement to kill those who opposed the religion. During the ensuing posts it was clear that most forum members said OBL4Caliph was wrong. However his language and argument were more structured to a youth's mind and he began to try and convince Hussein. While clearly Hussein had used the Internet for a sensible and reasonable purpose, canvassing views of like-minded people about his thoughts as a confused teenager, he had inadvertently shown a little potential in his thought, which led to grooming as a potential terrorist.

Fighting Radicalization

Whatever the reasons people have for becoming more radical, it is important that it is thoroughly understood in order to find a way of combating it. There is a deep mistrust of official communications by some elements of society and for others the messages are not received. It is no use planning the world's best programme to combat radicalization and then end up missing the target audience. It is also vital to listen to what is being said by those trying to radicalize others and how it is being said. New media such as Twitter and Facebook must be used where appropriate as they are thoroughly embraced by many terrorists. The British CONTEST[14] policy aims to combat radicalization in it's PREVENT work stream.

The United Kingdom's strategy for countering international terrorism was established in 2003 and is known as CONTEST. Details of the strategy were first published by HM Government in July 2006 and CONTEST 2, the updated strategy, was published in March 2009. It is an integral element of the UK's National Security Strategy published for the first time in March 2008. CONTEST consists

[13] Marc Prensky coined the term 'Digital Native' in his work "Digital Natives, Digital Immigrants" published in 2001. In his article, he assigns it to a new group of students enrolling in educational establishments. The term draws an analogy to a country's natives, for whom the local religion, language, and folkways are natural and indigenous, compared with immigrants to a country who often are expected to adapt and begin to adopt the region's customs. Prensky refers to accents employed by digital immigrants, such as printing documents rather than commenting on-screen or printing out emails to save as a hard copy. Digital immigrants are said to have a "thick accent" when operating in the digital world in distinctly pre-digital ways, for instance, calling people into a room to see a webpage instead of sending them the URL. For example a digital native might refer to their new "camera" but a digital immigrant might refer to their new "digital camera."

[14] CONTEST; PERSUE, PREVENT, PROTECT, PREPARE. The United Kingdom's Strategy for Countering International Terrorism, March 2009.

of 4 Work Streams – PURSUE, PREVENT, PROTECT and PREPARE. The aim of CONTEST is:…to reduce the risk to the United Kingdom and its interests overseas from international terrorism, so that people can go about their lives freely and with confidence

The PREVENT work stream is the United Kingdom's approach to tackle the causes of radicalisation through a better understanding of them. It has five main objectives:

1. to challenge the ideology behind violent extremism and support mainstream voices,
2. disrupt those who promote violent extremism and support the places where they operate,
3. support individuals who are vulnerable to recruitment, or have already been recruited by violent extremism,
4. increase the resilience of communities to violent extremism, and
5. to address the grievances which ideologues are exploiting.

The PREVENT strategy looks at forming partnerships with communities and representative groups to target and address the reasons people may be drawn to extreme or Al Qa'ida style views. It has brought together leaders and scholars to promote the mainstream views and to challenge ideologues within the community. It is understood that there are perceived grievances within some communities in the United Kingdom over foreign policy, specifically the United Kingdom's involvement in Iraq and Afghanistan, as well as social and political problems at home. This is being tackled by the PREVENT workstream to counter the extremist version of events. In partnership with faith and community leaders, the mainstream voice is being raised through a series of government-funded workshops, road shows and other educational means. Incorporating such partnerships with those mainstream leaders of the communities most likely to be vulnerable to extremism is vital. This is conducted at both local and national levels.

The role of the police is an important facet of PREVENT. Community police initiatives have been established to tackle individuals who are promoting violence and involved in recruiting for extremist organizations and target the areas in which they operate. In 2008, some 300 staff members were dedicated to work on this initiative. There is also an important international dimension to PREVENT. The threat of international terrorism can come from foreign nationals and British citizens who have attended radicalization and training camps overseas. The Government of the United Kingdom works with foreign governments in areas where such camps do or may exist, as well as with diaspora communities in the United Kingdom to help understand and resolve issues. Various initiatives have been introduced to challenge the ideology behind violent extremism which works alongside scholars and faith groups to develop positive alternatives to extremist ideologies. These are also at regional and local, as well as national levels, to engage those vulnerable to extremism.

Vulnerability occurs for many reasons, it is not just an attraction to a certain ideology but social, family and community concerns or pressure may compel people towards such a view. Many new programs have been introduced to address these and provide accurate information about the United Kingdom's foreign policy when it is grossly misrepresented by ideologues.

This aims to encompass all aspects of radicalization, including an understanding of the authorities when it comes to their actions.

Conclusions

There is a saying: "to stop being bitten by a mosquito, do not swat the mosquito but drain the swamp." This is true of terrorism in many ways. Terrorism is the ultimate form of politics, changing government policy or coercing society through fear and violence rather than debate and democracy. The solution to a terrorist situation is political and the cause must be understood to be defeated. However, it is important to stop the flow of terrorist recruitment and one of the early aspects of this is the radicalization of an individual.

The Internet has provided a new medium for radicalization. It is easier for young people to chat in order to post questions and get answers. However, it is also easier for a terrorist recruiter to pump false information into vulnerable people. And as they do not actually meet, the recruiter can pose as something he or she is not.

Terrorists also can make propaganda easily accessible. They can edit video and comment to produce an effect that suits their cause even though it is completely manufactured and not authentic. Mainstream media would be unlikely to fall for such propaganda. Those engaged in the fight against terrorism must understand what is being said and how people are accessing it. The terrorists have become expert, not only in using the latest tools of Internet communications, but to do it in a way that can shield their identities and even their locations. There is no use in just saying a terrorist message is wrong and giving out the correct information if it is in a format or medium the target audience does not use; it must also grab the interest of those it is aimed at. An unread piece of brilliance is no use. New and emerging methods of communication must be embraced. The Internet is a part of the battle space in the fight against terrorism and must not be ignored or used in such away that the terrorist message is read first. Often vulnerable people do not know who is telling the truth. It is these minds that must be convinced and won over in order to halt the supply of terrorist volunteers and therefore help strangle the terrorist organization.

References

Crenshaw, Martha, “The Causes of Terrorism,” Comparative Politics, Vol. 13, No. 4, July 1981, pp. 379-99.

Crenshaw, Martha, “Theories of Terrorism: Instrumental and Organizational Approaches,” Journal of Strategic Studies, Vol. 10, Issue 4, December 1987, pp. 13 – 31.

Stern, Jessica, “**Terrorism’s New Mecca,”** Op-Ed, Boston Globe*, 28 November 2003*.

The Madrid Summit Working Paper Series – Volume 1: Causes of Terrorism (2005).

Sageman, Marc, “Leaderless Jihad, Terror Networks in the 21st Century,” University of Pennsylvania Press (2008).

Note for Contributors

The *Defence Against Terrorism Review* (DATR) is an inter-disciplinary, biannual journal, publishing in-depth analyses of the complex issue of terrorism in a changing and globalised security environment. It includes political, legal, sociological, economic, and psychological approaches to the terrorism predicament. DATR intends to reach academics as well as practitioners and aims to publish theoretical as well as policy papers. It also encourages contributions from different cultural perspectives.

Manuscripts submitted to DATR should be in the environs of 8,000 words and must be written in English. Each paper is screened at COE–DAT and then sent to referees for reviewing.

Manuscripts must be typed in 12 puntos and double spacing with *Times New Roman* font, and should be sent directly to the Editor-in-Chief (acad@coedat.nato.int) *or* Assistant Editor (datr@coedat.nato.int) by e-mail.

Manuscripts should be organized as the title page, an Abstract (around 200-300 words), and Keywords (up to 5), Footnotes, and a Bibliography as shown below:

Footnotes

1. Mustafa Kibaroğlu and Ayşegül Kibaroğlu, *Global Security Watch – Turkey: A Reference Handbook,* Praeger Security International, Greenwood Publishing Group, Westport, Connecticut, USA, 2009, pp. 87-109.

2. Monica Den Boer, "The EU Counterterrorism Wave: Window of Opportunity or Profound Policy Transformation?" in Marianne Van Leuween (ed.), *Confronting Terrorism. European Experiences, Threat Perceptions and Policies*, Kluwer Law International, The Hague, 2003, p. 196.

3. Michael Doran, "Somebody Else's Civil War", *Foreign Affairs*, Vol. 82, No. 1, 2002, p. 32.

4. European Commission, Proposal for a Council Framework Decision on the European Evidence Warrant for Obtaining Objects, Documents and Data for Use in the Proceedings in Criminal Matters, Brussels, 11 November 2003 (http://eur-lex.europa.eu/LexUriServ/site/en/com/2003/ com2003_0688en01.pdf).

References

Den Boer, Monica "The EU Counterterrorism Wave: Window of Opportunity or Profound Policy Transformation?" in Marianne Van Leuween (ed.), *Confronting Terrorism. European Experiences, Threat Perceptions and Policies*, Kluwer Law International, The Hague, 2003, pp. 185-206.

Doran, Michael, "Somebody Else's Civil War", *Foreign Affairs*, Vol. 82, No. 1, 2002, pp. 22-42.

European Commission, *Proposal for a Council Framework Decision on the European Evidence Warrant for Obtaining Objects, Documents and Data for Use in the Proceedings in Criminal Matters*, Brussels, 11 November 2003 (http://eur-lex.europa.eu/LexUriServ/site/en/com/2003/ com2003_0688en01.pdf).

Kibaroğlu, Mustafa and Ayşegül Kibaroğlu, *Global Security Watch – Turkey: A Reference Handbook,* Praeger Security International, Greenwood Publishing Group, Westport, Connecticut, USA, 2009.

COE-DAT