C·A·P Center for Applied Policy Research

The Threat of Cyber Terrorism and Recommendations for Countermeasures

by Mayssa Zerzri

C·A·Perspectives on Tunisia No. 04-2017

This paper has been published as a result of the program "Policy Advice and Strategy Development", conducted by the Center for Applied Policy Research (C·A·P) in cooperation with the Union des Tunisiens Indépendants pour la Liberté (UTIL), the Arab Institute for Human Rights (AIHR) and the Faculty of Legal, Political, and Social Sciences of the University of Carthage. The program is part of the "Bavarian-Tunisian Action Plan 2016-2018" that the government of the Free State of Bavaria implements in cooperation with the Ministry of Development, Investment and international Cooperation of the Republic of Tunisia.

PROJECT SUPPORTED BY BAYERISCHE STAATSREGIERUNG

The Threat of Cyber Terrorism and Recommendations for Countermeasures

by Mayssa Zerzri

SUMMARY

Terrorist organizations have invaded cyberspace and made it a battleground. They no longer rely on military force such as weapons, armor and bombs only. Instead, they become more and more savvy, and their strategies and tactics have technological orientation. Moreover, their activities are no longer limited to propaganda, fundraising, training, planning and execution of physical attacks. Rather, they extended their field of action to attacking their victims by sabotaging online infrastructure from anywhere in the world in a way that hides their actual identity by the means of Inter- and Dark Net technology, therefore creating a new demand for adequate preparedness and countermeasures.[1]

This paper aims to shed the light on the legal, institutional and political challenges to address the phenomenon of cyber terrorism and to minimize its risks and consequences in the Tunisian context.

1. DEFINING CYBER TERRORISM

Cyber terrorism is the convergence of cyberspace and terrorism and it is different from cybercrimes, such as data theft, bank fraud etc. It is generally understood as an act that is

- executed via cyberspace by individuals, groups or organizations who are directly influenced by some terrorist movements or/and its leaders;
- motivated by a desire to effect political or ideological change;
- leading to violence that reaches physical and psychological repercussions beyond the immediate victim or target.

In order to develop an approach to fight cyber terrorism effectively, two main forms of this terrorist threat must be differentiated: 1. Hybrid cyber terrorism and 2. pure cyber terrorism.

2. CYBER TERRORISM IN ACTION

2.1 Hybrid Cyber Terrorism

Hybrid cyber terrorism is the use of the Internet for terrorist activities such as propaganda, recruitment, radicalization, fundraising, data mining, communication, training, and planning for actual terrorist attacks.

a) Propaganda and Psychological Warfare:

The Internet is being used by terrorists and terrorist organizations to spread and manage their propaganda through information warfare, to impart their ideology, to conduct psychological warfare as well as to radicalize and recruit new members from all over the world, through terrorist websites, online magazines, and various social media platforms (such as Facebook, Twitter, Instagram, Tumblr, VKontakte, JustPaste.it, Youtube, etc).

For instance, DAESH (or the so called Islamic State) had seven media agencies under its central media command (with Amaq being the most prominent one) and 37 media offices operating in various countries. Similarly, al-Qaeda formed a media arm known as As-Sahab and The Global Islamic Media Front (GIMF), as well as online magazines such as “Inspire and Resurgence” to reinforce their propaganda.

In addition, terrorist organizations have been using the Telegram application since the end of 2015 due to its encryption and secure use, and because of the increased closure of terrorist accounts on Facebook and Twitter.[2] In August 2016, for example, the Al-Sumud jihadist media institution, in support of DAESH propaganda, published on its Telegram channel links to download two anthologies containing a collection of the organization’s publications in Somalia and the Maghreb. Or, the “Orlando Channel – Omar Mateen” Telegram channel included publications encouraging Muslims in the West to carry out lone wolf attacks by allowing visitors to download a computer pro-

[1] Note that cyber terrorism is transnational and affects states and societies regardless the terrorists’ geographic location. Terrorist attacks can emanate from anywhere in the world.

[2] However, although being considered losing its control over territories in Syria and Iraq, DAESH state has demonstrated its resilience in maintaining constant distribution of its propaganda and its adaptability towards online removal of jihadist content, according to its affiliated outlet Yaqeen Media.

gram that contains videos, as well as official and semi-official articles by the Islamic State and its supporters, regarding the massacre in Orlando.

Also, to conduct psychological warfare, we can list examples such as the United Cyber Caliphate which is identified with the Islamic State and is part of the Islamic State Hacking Division, and which in July 2016 distributed several posters threatening the US and Egypt.

b) Communication and Networking:

Terrorists groups have used social media platforms (like Telegram) and encrypted messaging system applications (such as Kik, SuperSpot, Wickr, Whatsapp, Gajim), online gaming chat rooms, coded messages or steganography for covert discussions, direct and private communications purposes (that includes networking with other members of the group, interaction with recruits and supporters) and planning and coordination of physical attacks as well as planning hacking operations. For instance, VoIP phone services were used during the Mumbai attacks in 2008.

c) Fundraising:

Funding for terrorist related activities (acquire weapons or support the war effort by providing funds to the families of fighters) is no longer simply done through charity organizations. Instead, it is also being done by donation through social media platforms and blogs, and the use of the bitcoin digital currency. For instance, Indonesian security forces discovered a financial transfer made by an IS operative to another one in Indonesia using the bitcoin digital currency.

Other examples for fundraising campaign through social media platforms are

- The “Arm Us” campaign by which funds were declared to be directed to “Jihad for Allah”, arm mujahidin with weapons and munition, manufacturing weapons and missiles and bombs, physical training, promoting sharia and dawah (proselytisation), establishing jihadi propaganda, as well as developing and providing security and community activity.

- The “Your Sons at Your Service” fundraising campaign which, for example, captioned a plan to sponsor a mujahid family with 100$ per month.

d) Data Mining, Recruitment and Training:

Terrorists are using the Internet for data mining to collect information of particular places and individuals as potential targets for attacks as well as recruitment. Already in the case of the attacks of 11 September 2001, the al-Qaeda operatives used the Internet to collect information such as flight times and to share information and coordinate their attacks.

Today, DAESH and many other organizations are utilizing social media platforms to select individuals for radicalizing or recruitment purposes. Recruiters identify potential targets by monitoring Facebook profiles and conversation threads and assess whether they are genuine sympathizers. They conduct further examination by adding them as friends and only engage in private communication only after they are certain of the individuals’ faithfulness.

Finally, terrorist organizations use the Internet and especially the Dark Net to disseminate training materials to conduct physical attacks, and distribute guidelines and instructions to equip their members and supporters with the necessary skills in order to support their cyber defense and to improve their offensive capabilities.

2.2 Pure Cyber Terrorism

Pure cyber terrorism refers to direct attacks on a victim’s cyber infrastructure (such as computers, networks, and the information stored therein) to achieve the political, religious and ideological objectives. Destructive and disruptive cyber terrorism can be further differentiated:

- Destructive cyber terrorism is the manipulation and corruption of information system functions to damage or destroy virtual and physical assets. The most popular weapon is the use of computer viruses and worms; trojans and ransomware.

- Disruptive cyber terrorism is described as hacking designed to take down websites and disrupt the normal lifestyle, which relies on critical infrastructure supporting medical utility, transportation, and financial systems.

Thus, in recent years, several groups of pro-DAESH hackers have been active in hacking web hosts to deface internet sites, spreading religious extremist propaganda and open calls for cyber warfare on social media, as well as in harming online services and businesses. In order to boost their hacking capabilities as well as to strengthen their position in the cyberspace, some of them have merged (such as the so-called Ghost Caliphate Section, the Sons Caliphate Army, the Caliphate Cyber Army and the Kalashnikov E-Security into the so-called United Cyber Caliphate). A number of the following examples that occurred in 2015 illustrate the threat of cyberattacks to the stability of the global economy, transportation and information, and to world peace:

- The Fallaga, a Tunisian hacker group who is linked to DAESH, attacked and defaced several websites belonging to the British Ministry of Health during a defacement attack, replacing legitimate webpages with photos from the war in Syria, and included messages such as "Stop the Killing in Syria" and hashtags such as #Op-Russia or #Save-Aleppo;

- Another DAESH-related hacker group, called AnonGhost, hacked the Facebook and Twitter accounts of the Royal Malaysian Police (RMP) by changing the profile photo and cover image;

- The United Cyber Caliphate hacker group, which is also identified with the DAESH, once published a video calling on Muslim hackers to use their hacking abilities to help in the battle against infidel countries. In another incident, the group claimed responsibility for the breach of the Facebook page and the Telegram channel "Raqqa is being Slaughtered Silently", which collected news items regarding crimes carried out against the civilian population in Syria, notably by DAESH.

- The Cyber Caliphate hacking group managed to hack the Malaysia Airlines website and to take control and deface the French TV5 broadcaster and TV station's eleven channels' Twitter, Google+ and Facebook accounts, websites etc. The group broadcasted DAESH propaganda and made references to the attack on Charlie Hebdo. In the very same year, the group managed to hack into the US military Central Command (CENTCOM)'s Twitter and YouTube accounts.. During the attack, CENTCOM's Twitter account's icon was replaced with an image of a masked man along with the words "Cyber Caliphate" and "I Love You ISIS" whereas on CENTCOM's YouTube page they posted two pro-DAESH videos. More seriously, the hackers were able to post personal information of 4-Star US generals including their names, telephone numbers and home addresses.

So far, Jihadist terrorist organizations and groups are working to improve their cyber offensive and defensive capabilities exploiting the availability of cybercrime tools and services on underground criminal markets. They also attempt to intensify their online activities focusing on disseminating propaganda to attract even more recruits and funding. To date, they have only been able to deface websites and make minor hacking cases. However, it is only a matter of time before these terrorist organizations will recruit and/or contract more experienced cybercriminals and buy more advanced technology enabling them to execute serious attacks with a greater negative impact.

3. TUNISIA: ASSETS, CHALLENGES AND RECOMMENDATIONS

In recent years, Tunisia has succeeded in dismantling and neutralizing many terrorist cells and thwarting many subversion schemes in cooperation with international partners. Moreover, there have been ongoing national, regional and local efforts to counter terrorist threats and to dismantle financing networks linked to organized crime and extremism. In this regard, Tunisia has passed the Organic Law No. 2015-26 dated 7 August 2015 on the Fight against Terrorist Crimes and Repression of Money Laundering and developed a national strategy to fight extremism and terrorism.

The implementation and the proper functioning of the following legal mechanisms and institution are paramount to counter cyber terrorism effectively.

3.1 Legal framework

a) Existing Laws and Codes:

- Organic Law No. 2015-26 of 7 August 2015 on the Fight against Terrorist Crimes and Repression of Money Laundering;

- Law No. 2008-01 of 8 January 2008 concerning the revision and completion of the Telecommunications Code promulgated by Law No. 2001-01 of 15 January 2001;

- Law No. 2005-51 of 27 June 2005, on electronic transfer of funds;

- Organic Law No. 2004-63 of 27 July 2004, on Protection of personal data (in process of update);

- Law No. 2004-05 of 3 February 2004 on computer security;

- Law No. 2000-83 of 9 August 2000 on electronic commerce;
- Telecommunication Code promulgated by Law No. 2001-01 of 15 January 2001;
- Budapest Convention on Cybercrime (Treaty No. 185) of the Council of Europe which can be considered the international reference framework).

b) Laws and Codes sui generis:

- Law on the Fight against Cyber Crime;
- Digital Code.

3.2 Institutional capacity

a) Executive mechanisms:

- National Counter-Terrorism Commission;
- Tunisian Commission of Financial Analysis;
- Ministry of the Interior;
- Fusion Centre for the Fight against Terrorism and Organized Crimes;
- Ministry of Communication Technologies and Digital Economy;
- Technical Agency of Telecommunications;
- National Agency for Computer Security;
- Tunisian Internet Agency;
- National Digital Certification Agency;
- Ministry for Relation with Constitutional Institution, Civil Society and Human Rights;
- National Instance of Personal Data Protection.

b) Judicial mechanisms:

Judicial courts:

- Courts of First Instance / the Counter Terrorism Judicial Pole;[3]
- Courts of Appeal;
- Court of Cassation.

Military Justice:

- Permanent Military Tribunal of 1st Instance of Tunis;
- Military Court of Appeal.

Taking into consideration all the efforts undertaken to govern the area of information and communication technology, some more major shortcomings to prevent cyber terrorist acts from occurring and/or to safeguard citizens and human rights, including those of the presumed terrorists, must be noted here:

- The non-compliance of many public structures with the legal and regulatory measures in this area represents a serious threat that can benefit terrorists to penetrate information systems.[4]
- In the context of open government, there is a lacking framework to adjust the classification of sensitive data, such as those on critical infrastructures, and the problem of the non-dissemination of data to the new kinds of threats posed by cyber terrorists as presented in this paper.
- The absence of a framework that regulate the use of social media networks by citizens as well as government agencies to track and monitor terrorist organizations or individuals; it must be noted, however, that any regulation can constitute a restriction of the freedom of the Internet represented by access, freedom of expressions and information, privacy and data protection.

3. RECOMMENDATIONS

In order to counter the ill-effects of cyber terrorism on critical infrastructures and businesses as well as the social and psychological effects that these attacks have on citizens, a multidimensional and comprehensive strategic approach should be put in place:

[3] According to the Fight against Terrorist Crimes and Repression of Money Laundering Law, the Court of First Instance of Tunis, through the judges appointed to the Counter Terrorism Judiciary Pole, is competent, without other judicial or military courts over terrorist offsets under this Act and related obligations if they were committed in the Tunisia.

[4] See also the statistics related to audit of information systems security, completed during the years 2010-2015 by public and private institutions and published by the National Agency for Computer Security; https://www.ansi.tn/fr/pages/statistics/years/audit.html.

3.1 Legislative Framework

- Enact an Internet regulation with respect to the various threats posed by cyber terrorism; including the monitoring of social media platforms in order to detect, respond and deter any possible spreading of terrorist propaganda, radicalization communications between individuals and known terrorist elements, activities of data mining for the purpose of planning terrorist attacks or recruitment of individuals and other terrorist related Internet usages; as well as monitoring terrorist activities in the Dark Net. Adequate mechanisms ensuring respect the freedom of expression and privacy must be developed. Moreover, monitoring should be undertaken with consistency and integrity to target terrorists and others who pose a threat to national security.

- Develop a framework regulating Open Data to prevent activities of data mining for the purpose of planning terrorist attacks.

3.2 National Partnerships

- Strengthen cooperation between all stakeholders of the public and private sector, i.e. the government including security forces, cyber security experts, telecommunication network operators, internet service providers and civil society.

- Strengthen stakeholders‘ capacities (cyber security specialists, law enforcement agencies and the judiciary), as well as civil society by raising awareness regarding cyber security to prevent threats.

3.3 National Strategies

It has become indispensable to analyze cyber terrorism accurately, i.e. studying its objectives, motivation and the resources used; monitoring strategies and activities; and analyzing and evaluating risks for damage they could cause.

In parallel it is necessary to formulate several national strategies, such as:

- a National Cyber Security Strategy that aims to develop and enhance cyber security in Tunisia to be secure and resilient to cyber threats. The strategy must outline the objectives and the implementation plan to help create the conditions for all stakeholders to work effectively on cyber security, and raise the level of awareness and knowledge throughout the society;

- a National Response and Risk Management Strategy to identify and characterize cyber threats, assess the vulnerability of critical assets to those threats, determine the risk, identify ways to reduce those risks and prioritize risk reduction measures;

- an holistic National Communication Strategy to enhance trust between citizens, security forces and media;

- a National Strategy to Counter Terrorist Online Propaganda as terrorists remain resilient in maintaining constant distribution of its propaganda and its adaptability towards online removal of jihadist content.

3.4 International Cooperation

- Coordinate action and conclude agreements with other states regarding crimes related to cyber terrorism (including information exchange to prevent cyber terrorist operations);

- Regulate the prevention and treatment of this crime and the exchange of information and evidence. This will include the activation of extradition agreements for cybercrime offenses;

- Promote the exchange of information, best practices and lessons learnt between states in preventing and countering cyber terrorism.

Author and contact
Mayssa ZERZRI
Cyber Security Expert
Holder of a Master‘s Degree on
Information Systems and Networks Security
Certified Auditor on Information Systems’ Security -
National Agency for Computer Security
Certified Cobit5 Foundation - APMG International
zerzri.mayssa@gmail.com