Chapter 19

Prevention of (Ab-)Use of the Internet for Terrorist Plotting and Related Purposes

Branislav Todorovic and Darko Trifunovic

The internet has become an indispensable tool for human communication, offering an abundance of information and a great variety of applications. However, the worldwide web also offers ample opportunities for malefactors (e.g., criminals, terrorists, demagogues) to carry out activities cause serious damage. Due to the internet's wide-reaching nature, any investigation of its (ab)use has to be defined in terms of boundaries. This chapter addresses the (ab)use of the internet for terrorist activities and seeks to provide useful information to detect and address this issue. In doing so, this chapter covers five issues:

- Terrorist group's employment of social media platforms to recruit new members and communicate with their sympathizers. This chapter explores possible ways to detect, mark, and suppress such activities (e.g., secret encrypted communication, internet deep search software, human-machine interaction, and new generation artificial intelligence tools).
- Terrorist organizations also utilize the internet for propaganda purposes. Based on various examples, this chapter analyses patterns in publications and advertisement of 'heroic' terrorist activities, which, in turn, can be useful for anti-terrorist campaigns.
- The internet has proven to be a valuable marketing and public relations medium for terrorism funding purposes.
- Terrorists (ab)use on the internet publicly available information (i.e., by means of data mining) to plan, and carry out attacks. This chapter offers suggestions of measures that can be used for prevention and preparedness.
- Terrorists thrive well on the internet because it anonymously accessible. This chapter explores options and tools for tackling this anonymity (e.g., with the help of behavioral statistics).

The analyzed forms of use/abuse of the internet by terrorists are classified and structured by type and purpose. Possibilities for prevention are discussed for each group or cluster.

Keywords**:** internet, terrorist activities, prevention, preparedness, propaganda, recruitment.

The title of this chapter might also be "the prevention of the exploitation of the internet for terrorist plotting and related purposes."[1] In this chapter we will highlight recent developments and limitations of the contemporary methods to prevent and dismantle harmful activities. In addition to this, we will do the following:

- Determine which activities on the internet fall under the category of terrorist plotting and related purposes;
- Create a proper systematization of such activities for further analysis; and
- Provide a comprehensive list of preventive measures.

To begin with, one has to always keep in mind that the (ab)use of the internet for terrorist plotting covers a very broad area, corresponding to the general use of the internet. If a definition of 'prevention' would be applied literally (e.g., the one of the Cambridge Dictionary which defines it as "the act of stopping something from happening or of stopping someone from doing something"[2]) that might be understood as being possible to intercept the (ab-) use of the internet by terrorists with a high degree of probability. That, however, is not true in most cases, though it is possible to prevent terrorists from abusing certain features of the internet. In reality, it is more probable that counterterrorism professionals manage to detect and identify terrorist plotting activities that are already underway; they can then prevent these plots from evolving into actual operations, or at least limit some of the possible damage. It might also be possible to prevent further escalation or contagion in the form of copycat acts.

The first to define terrorist activities on the internet. This is a challenging task, as some activities are only partially related to the internet; with the example of so-called cyberterrorism as the most characteristic one. Due to a rapid and broad development of Information Technology (IT) and cyber systems since the early 1990s, cyber security has become a major topic on its own, with cyber attacks and their prevention being just one segment. Therefore, the derived systematization presented below will have to undergo further deliberation and adjustments before reaching its final form.[3]

That the internet provides terrorists with an extensive set of tools is undisputed. For example, the internet assisted Salman Ramadan Abedi in preparing his 2017 Manchester Arena suicide bombing:

> "According to the UK Parliament's Intelligence and Security Committee (ISC), 'access to extremist material online is reported to have been a key factor in the Manchester Arena attack which killed 22 people', referring to a newspaper report that the attacker, Salman Abedi, used YouTube videos to learn how to make his explosive device."[4]

However, the uses of YouTube cannot be curtailed just because someone (ab)used some of its content. Similarly, Google Earth as a tool is assisting a vast number of people on an every-day basis. This is to say that the possibility that terrorists use Google Earth to examine the locations , should not and will not stop Google Earth to operate for the common good (and for the company's profits).

This raises the question of how to effectively prevent, or at least significantly reduce, internet (ab)use, while maintaining bona fide use. It is often difficult to separate benign and hostile internet users, while also taking into account privacy concerns, and respecting freedom of expression .To cope with the vast amount of information on the internet, there are automatic tools available that can push, remove, or block (access to) content. Occasionally, information is stored unnecessarily on the internet. Without any aspiration to take sides, we present two examples that indicate that these issues need a great deal of attention. Take, for instance, this news report:

> "The UK government is trying to restrict access not only to the terrorists' own channels, but also material hosted on the research website *jihadology.net*, stating that it is 'reckless to publish terrorist propaganda online without safeguards to stop those vulnerable to radicalization from seeing it'. As a result, what looks like a double standard has emerged. In February 2015, for example, Fox News in the US broadcasted excerpts of one of the most notorious items of terrorist propaganda ever produced: the last moments of Moaz Al-Kasasbeh, a Jordanian fighter pilot captured by Daesh (also known as the Islamic State of Iraq and Syria, ISIS) who was held in a cage and burned to death. To this day, Fox News continues to host the entire 22-minute video on its website – content which would undoubtedly have been removed by YouTube or Facebook."[5]

In this particular example, it is worth noting that the academic website *jihadology.net* was restored after an intervention of scholars who rely on it to study terrorist propaganda materials.

Review: Literature on Terrorist Use of the Internet

Technology is advancing fast in the digital field. Since the late 1980s, the internet has proven to be a highly dynamic vehicle for communication, reaching now more than half of the global population. Technology is also a driving force for terrorist organizations and their supporters for a broad range of objectives. The internet has become a favorite tool for terrorists because of the many advantages it provides, including these: easy access, little or no regulation, weak or no censorship or other forms of governmental control, potentially huge audiences spread across the world; anonymity of communications, fast flow of information, interactivity, inexpensive development and maintenance of a web presence, a multimedia environment, and the ability to influence coverage in the traditional mass media.

Terrorist groups or their front organizations maintain their own websites to spread propaganda, raise funds, recruit and train members, communicate with their followers, and also prepare and sometimes even steer ongoing attacks. They also rely on email, chatrooms, e-groups, forums, virtual message boards, and resources like YouTube, Facebook, and Google Earth.

Fighting online terrorism is complicated and costly. The virtual war between terrorists and counterterrorism forces and agencies is a dynamic one. Rapid developments in technology represent both challenges and tools for global efforts to counter terrorism. While the many benefits of the internet are evident, its downsides are still underestimated when it comes to terrorism. [6] The misuse of internet-based tools for terrorist purposes represents a serious threat, since more and more essential aspects of contemporary society are almost completely dependent on the functioning of computer systems and the internet.

Preventing as well as investigating terrorist use of the internet requires adequate legislation and also effective technical solutions. These challenges differ largely from those identified in the fight against more traditional terrorist activity. As a result of the available network technology and the multitude of internet-based services, these challenges range from addressing the easy availability of instructions on how to commit terrorist acts to monitoring the use of encryption technology in terrorist communications.[7] As terrorist groups turn to technical tools to organize, plan, operate, finance and support their activities, their increasing reliance on technology also makes them more vulnerable to government agencies' intelligence collection. Governments are developing increasingly sophisticated techniques to identify and track potential terrorists. Rapid advances in technology also permit non-governmental organizations and researchers to detect and monitor many of the online activities of suspected terrorists in cyberspace. Thousands of suspected terrorist websites have been catalogued by various entities around the world. Interlinks between forms of organized crime and terrorism

have been discovered and exposed. Terrorist organizations and organized crime groups often use similar tactics- so much so that that distinguishing between what is a non-political 'criminal' and a political 'terrorist' act can be a difficult task. On the other hand, many legal and police responses to terrorism parallel approaches to countering organized crime.[8]

The development of increasingly sophisticated technologies has created a network with a truly global reach, and relatively low barriers for entry. Internet technology makes it easy for an individual to communicate with relative anonymity, quickly and effectively across borders, enabling him or her to reach an almost unlimited audience. The benefits of internet technology are numerous, starting with its unique suitability for sharing information and ideas.[9] It must also be recognized, however, that the same technology that facilitates freedom of communication can also be exploited for the purposes of terrorism. The following section explores this in more detail. It is partly based on the findings of a report prepared by the UN Office on Drugs and Crime.[10]

Methods and Purposes of Internet Use for Terrorist Objectives

When it comes to terrorist abuses of the internet, it is possible to identify six sometimes overlapping categories: propaganda (including recruitment, radicalization and incitement to terrorism); financing; training; planning (including through secret communication and open-source information); execution; and cyber attacks.

1. Propaganda: Contemporary propaganda generally takes the form of communications providing ideological explanations, listing grievances and offering justifications for the promotion of terrorist activities. Such propaganda may include textual messages, visual presentations, glossy magazines, religious treatises, audio- and video-music and movie files as well as video games developed by terrorist organizations or their supporters and sympathizers. What constitutes terrorist propaganda - as opposed to legitimate advocacy of a political perspective - is often difficult to determine. In general, propaganda involves the selective and manipulative dissemination of biased information, mixing (half-)truths and lies and appealing in emotional ways to latent widespread prejudices in order to encourage action against political opponents. The promotion of violence is a common theme in terrorism-related propaganda. Terrorist propaganda distributed via the internet covers a range of objectives. It may also be used to showcase the effective execution of terrorist attacks to those who have provided financial support. Other objectives of terrorist propaganda may include the use of psychological manipulation to create a sense of heightened anxiety, fear or panic in a population or subset of it. This may be achieved through the dissemination of disinformation, rumors, threats of violence or images relating to violence.

1.1. *Recruitment*: The internet may be used also as a way to develop relations with, and solicit support from, those held most responsive to targeted propaganda. Terrorist organizations increasingly use propaganda distributed via platforms such as chat groups as a means of clandestine recruitment.[11] The reach of the internet provides terrorist organizations and sympathizers with a global pool of potential recruits. Restricted access cyber forums offer a venue for those initially recruited to learn more about, and provide support to, terrorist organizations and, ultimately, to engage on their own in direct actions in the furtherance of terrorist objectives.[12] Propaganda may be fine-tuned and adapted to account for demographic factors, such as age or gender, as well as social or economic circumstances. Some terrorist organizations have even designed online video games intended to be used as training tools. Such games may lower the threshold of individuals to use violence in real life and promote the use of violence against specific political leaders. Some of these games are offered in multiple languages to appeal to diverse audiences.[13]

1.2. *Incitement:* The internet provides an abundance of material and opportunities to download, edit and redistribute content that may be considered unlawful glorification of, or provocation to, acts of terrorism. The line between information and influence operations can be a thin one. Media censorship has increased in authoritarian states. However, for democracies governed by the rule of law, restrictions on the exercise of the right to freedom of expression have to be both necessary and proportional to the threat posed. The right to freedom of expression is also linked to other important rights, including the rights to freedom of thought, conscience and religion.[14] Closing down open societies in order to stop incitement to violence by fringe groups in society is not the right answer.

1.3. *Radicalization:* Incitement, radicalization, and recruitment to terrorism may be viewed as points along a continuum. Radicalization refers primarily to a process of indoctrination that ideologically socializes or converts young people to an extremist worldview and mobilizes them to support, and ultimately perform, acts of violence against designated political opponents. The process of radicalization generally involves the use of propaganda, whether communicated in person or via the internet. The length of time it takes to win recruits depends on the effectiveness of the propaganda and on the mix of individual and social push and pull factors of vulnerable recipients.

2. Financing: Terrorist organizations and supporters also use the internet to raise money for acts of terrorism. They do so in four different ways: direct solicitation, e-commerce, the exploitation of online payment tools and through charitable organizations. Direct solicitation refers to the use of websites, chat groups, mass mailings and targeted communications to request donations from supporters. Websites may also be used as online stores, offering books, audio and video recordings and other items to supporters. Online payment facilities offered through dedicated websites or communications platforms make it easy to transfer funds electronically between parties. Online payment facilities may also be exploited by terrorists through fraudulent means such as identity theft, credit card theft, wire fraud, stock fraud, intellectual property crimes and auction fraud. Financial support provided to seemingly legitimate organizations, such as charities, may also be diverted for illicit purposes. Some terrorist organizations have been known to establish shell corporations, disguised as philanthropic undertakings, to solicit online donations. These organizations may claim to support humanitarian goals while in fact much or all of the donations are used to fund acts of terrorism.[15]

3. Training: Since practically all terrorist organizations lack permanent territorial safe havens, many of them have increasingly turned to the internet as a virtual training ground. There is a wide range of media that provide platforms for the dissemination of online training manuals and bomb making information. These platforms are used to share specific methods, techniques or operational knowledge for the purpose of committing acts of terrorism.[16]

4. Planning: Many criminal justice practitioners have indicated that almost every new case of terrorism prosecuted involved the use of internet technology. In particular, planning an act of terrorism typically involves remote communication between several conspirators.

4.1. *Preparatory secret communication:* The most basic function of the internet is to facilitate instant communication. Terrorists have become increasingly sophisticated at exploiting communications technologies. A simple online e-mail account may be used by terrorists for electronic "dead dropping" of communications. This involves the creation of a draft message, which remains unsent. It leaves minimal electronic traces but may be accessed from any internet terminal worldwide by multiple individuals in possession of the relevant password. There is also an abundance of sophisticated technologies that increase the difficulty of identifying the originator, the recipient or the content of internet

communications. Encryption tools and anonymizing software and steganography are readily available online for download.[17]

4.2. *Publicly available information:* Organizations and individuals publish extensive amounts of information on the internet. In the case of organizations, this may be a result of a desire to promote their activities and broaden their interactions with consumer in general. Particularly in the age of popular social networking media, such as Facebook, Twitter, YouTube, Flickr and blogging platforms, individuals also publish, voluntarily or inadvertently, an unprecedented amount of potentially sensitive information on the internet, often without considering how it can be used against them.

5. Execution: The use of the internet in furtherance of the operational execution of acts of terrorism offers logistical advantages, while the likelihood of detection and arrest is low as double encryption allows the hiding of the identity of senders and receivers. Internet purchases may facilitate the acquisition of items necessary for the execution of terrorist attacks (e.g., chemicals needed for bomb-making). Stolen credit card information or other forms of compromised electronic payment tools may be used to finance such purchases.

6. Cyber attacks: A cyber attack generally refers to the deliberate exploitation of computer networks as a means to penetrate more or less protected networks. Such attacks are typically intended to disrupt the proper functioning of targeted computer systems, servers or underlying infrastructure, by means of use hacking, viruses, malware or other means.[18]

Methods to fight cybercrime in general and terrorist use of the internet in particular currently attract a great deal of attention. The reason for this is not just that some of the methods are new and therefore require intensive research, but also that the investigation of crimes involving network technology presents particular difficulties. Effective investigations relating to internet activity rely on a combination of traditional investigative methods, knowledge of the tools available to conduct illicit activity via the internet and the development of practices targeted to identify, apprehend and prosecute the perpetrators of such acts – criminals and terrorists or government agents who are often in another country than where the attack took place. A proactive approach to investigative strategies and supporting specialist tools that capitalize on evolving internet resources enables better identification of data and servers and is likely to yield greater benefits to investigators.

There is a range of specialized utilities and hardware available to investigators with the appropriate technical background and security clearances. Due care should be taken, where possible, in cases involving the acquisition of digital evidence to implement standardized data recovery procedures to promote the retrieval of all the available evidence and the preservation of the integrity of the data source so as to ensure admissibility of evidence in court proceedings. Owing to the fragile nature of digital evidence, its examination is best performed by specially trained forensic experts.

Effective international cooperation is an important factor in many terrorism-related prosecutions. States are legally obliged, under various multilateral and bilateral legal instruments related to terrorism and transnational organized crime, to establish policies and legislative frameworks to facilitate effective international cooperation in the investigation and prosecution of acts of terrorism and serious organized crime. However, there is often a long way to go between legal obligations regarding mutual judicial assistance and the honoring of requests for arrest and extradition of criminals and terrorists abusing the internet in third-party jurisdictions.

Key Aspects of the (Ab-) Use of the internet for Terrorist Plotting

In this chapter we propose a new system for the categorization of the (ab-) use of the internet for terrorist plotting. It is firstly grouped by type (i.e., the method of internet (ab-) use and to which segments of internet it relates) and each derived cluster is further divided by purpose (sub-group). The main purpose is to discuss practical aspects of internet (ab-) use, with an emphasis on prevention. Grouping by type allows exploiting the common denominator among sub-groups within each cluster, which in most cases means that the same or similar preventive & countermeasures can be used for the whole cluster. The classificatory scheme can be used by other analysts by simply reorganizing the sub-groups into new clusters on the basis of selected criteria.

Main Types of internet (Ab-)Use by Terrorists (IAT stands for 'internet abuse type')

- **IAT1 -** Direct approach over internet (abuse of various means of communication, including mass e-mails, conference calls, etc.) and development of relationships
- **IAT2 -** Secret, encrypted, anonymous and similar communications
- **IAT3 -** Online multimedia materials
- **IAT4** - Dedicated internet tools; e.g., interactive websites (including specialized ones like e- commerce, undercover NGO or charitable organizations), chat-rooms, etc.
- **IAT5** - Social networking platforms
- **IAT6** -Video games and similar interactive means of promotion, downloadable from internet
- **IAT7** - Online payment tools (including cyber crime techniques)
- **IAT8** - Exploitation of publicly available information & resources
- **IAT9** - Cyber attacks

Division by purpose has been accepted as the following (SG stands for 'Sub-Group'):

- **SG1**- Propaganda
    - Recruitment
    - Incitement
    - Radicalization
- **SG2 -** Financing
- **SG3 -** Training
- **SG4 -** Planning
- **SG5 -** Execution
- **SG6 -** Cyber Attacks

General Preventive Measures

An important task is to provides training to staff from law enforcement and corresponding agencies fighting against terrorism. Main tasks can include:

- The detection, recognition and classification of internet-based terrorist activities.
- The use of automatic and semi-automatic tools for identification of internet-based terrorist activities.
- The verification of identified terrorist activities and application of preventive or countermeasures.

Although law enforcement agencies are at the forefront when it comes to the fight against terrorism, it is crucial to establish dialogue and enable cooperation between all relevant

government agencies and departments, as well as with the private sector in order to better prevent the (ab-) use of the internet by terrorist individuals and organizations. This requires all parties to establish in detail a common structure and methodology for fighting against terrorist (ab-) use of the internet.

Another key segment to prevent the (ab-) use of the internet for terrorist plotting is to put in place an adequate legal framework for action. The rule of law requires that the valid evidence is presented; in this case it includes the admissibility of digital evidence in counterterrorism cases in court. Since internet providers are mainly private companies, the issues of securing evidence may also require close cooperation between governmental and private institutions.

The (ab-) use of the internet by terrorists has significant implications for the private sector, in particular for those technology and social media companies whose products and services are used by millions, and these days even billions of people across the globe. While the companies in question have a business incentive to create a digital environment where their users feel safe, internet companies are increasingly compelled by governments to cooperate in blocking, filtering, countering or removing content or accounts based on public safety or national security considerations. In addition, internet users expect the service-providing companies to be transparent, accountable, respect privacy and freedom of opinion and expression, while also ensuring an open, free and secure internet – demands that can be conflicting with each other. Security concerns have led to greater voluntary engagement of the private sector in efforts to respond to terrorist (ab-)use of the internet. This engagement includes industry-driven initiatives and participation in multi-stakeholder and public-private fora focusing on normative, technical and organizational issues, as well as consultation with academic experts. Together, these efforts are hopefully resulting in the gradual emergence of a normative framework shaping private and public action in this area, based on a growing joint awareness of the scope of the problem. However, important challenges remain, including the fact that many industry actors are yet to fully engage while some governmental (over re-) actions can undermine trust in this progress.[19]

An example of coordinated activities in this area was the first course (2 to 6 July 2018) that was held under the auspices of INTERPOL's Project Trace, a three-year capacity building program funded by the government of Canada. With a clear focus on detecting, preventing, investigating and ultimately prosecuting terrorism-related crimes, participants learned how to collect, analyze and share information found online. The course was led by INTERPOL experts as well as partners from the International Centre for Political Violence and Terrorism Research (ICPVTR), the Financial and Technology Crime Division of Singapore, the Australian Federal Police, the US Federal Bureau of Investigation (FBI) as well as representatives from Facebook. This was followed by the first INTERPOL-United Nations Office for Counter-Terrorism (UNOCT) workshop on using information collected on social media to target Foreign Terrorist Fighters (FTF). The second session (9-10 July 2018), entitled "Enhancing Member State Capacities to use Social Media to Prevent and Counter the Foreign Terrorist Fighters Phenomenon" was funded by the government of Japan and UNOCT. Through practical exercises, it sought to deepen understanding of the FTF phenomenon via the collection of social media information with the aim to support counterterrorism investigations.[20]

General Countermeasures

It is very important to understand the motives and purposes of terrorist organizations in order to fight them. In practice, in particular when the (ab-) use of the internet for terrorist plotting is concerned, effective application of countermeasures requires knowledge of the instruments and methods terrorists use to further their goals. In that sense, some segments of the internet and web platforms are better suited for specific Internet Abuse Type (IAT) applications than

others. As the internet develops, and more people learn how to use it, so do terrorists adapt and adjust their (ab-) use of this global communication instrument.

Policymakers, in both government and corporate settings, and the wider counterterrorism policy research community must understand how terrorists use specific platforms in order to effectively prescribe countermeasures. For example, platforms used for content hosting should prioritize mechanisms to identify terrorist propaganda. To achieve this, various techniques for content matching are proving useful. However, some of these techniques will not be as important for platforms used to maintain a group's community, to communicate securely, and to organize financing. For those platforms, identifying behavioral signals or information-sharing with partners may be more important. Platforms that support numerous functions will need to develop a variety of countering techniques. There is no one-size-fits-all solution to this problem.[21]

Penetrating the Deep and the Dark Nets

With the growth of the internet (ab-)use by terrorists has also expanded. Systems that support prevention and counter actions against (ab-) use of the internet by terrorists, have to possess the ability to search, filter, adapt and transfer to its operational databases large amounts of data from the web for further processing – something called data injection. That data needs to be further processed, either by fully automated or by semi-automated tools - a process often called data mining. To achieve investigation objectives, counter-terrorism focused search engines need the capability of handling normal internet data, but should also be able to access data from the so-called deep and dark nets. Specific forms and tools applied for data processing depend on the type of internet (ab-) use by terrorists, as discussed above.

Direct Approach over Internet and Development of Relationships (IAT1)

This type of activity covers communications over the internet in open format (without encryption or attempts to conceal identities of participants). It covers all types of communication over the internet: e-mail; twitter; phone calls and messaging, i.e., voice over IP (VoIP) and instant messaging (IM) (e.g., Viber, WhatsApp, Telegram, WeChat, etc.); Although some of the communication channels claim to be secure by their providers (e.g., Viber or Telegram), they still belong to type IAT1 since there is no assured end-to-end encryption. While the basic encryption might be enough to protect web-based communications by ordinary listeners, it is not enough when hackers, specialists or providers themselves use their tools.

Due to the rather low level of security provided by many internet providers, terrorists and terrorist groups often conduct their communications in codes that do not raise suspicion among third parties. On the one hand that makes their communication more complex, slower and bound to errors, but, on the other hand, it does not draw the immediate attention of human counterterrorism-analysts and/or automatic conversation analysis algorithmic systems. In rare cases where speed is of essence, like when it comes to the execution (Sub-Group 5 or SG5) of terrorist attacks, terrorists might communicate without encryption. By counting on delayed detection and alert mechanisms and inertness among members of response teams, frequently combined with an optimistic view of chances for a fast escape (or, alternatively, a willingness to lose their own lives during the attack), some terrorists take the risk of open communication in the expectation to complete their attack actions and achieve their tactical goal as planned despite a high chance of being detected.

Internet Abuse Type 1 (IAT1) can be used for all subgroups, though in cases of propaganda (SG1) and financing (SG2) it is more often used after initial communication links had already

been established and communication in code was agreed upon. IAT1 is common for active recruitment in cases where direct personal contact does not require covert communication. With regard to recruitment (as part of SG1), type IAT1 is used as a simple and low-cost approach.

Preventive and Countermeasures

Internet Abuse Type 1 (IAT1) is commonly related to covert listening in on conversations or reading of e-mails and messages. While the beginnings of telephone-based mass surveillance dates back more than one hundred years, the situation has changed. Due to the immense number of continuous conversations, these are often captured and recorded and only later analyzed rather than in real time. Contextual search algorithms with machine learning and big data are coping well with traditional IAT1 type. When communication in codes is conducted, machine learning is of great assistance through pattern recognition and other algorithm enhancements. However, by the time intercepted communications are analyzed, the time for actionable preventive measures has in many cases already passed.

Advances made in the field of artificial intelligence, machine learning and big data also raise fundamental legal, ethical and cultural questions as to how these instruments and techniques should be used in counterterrorism. Used appropriately, these technologies are beneficial not only in the fight against cybercrime, but also for scientific research and education. However, at the same time these new tools present greater risks for malicious use and abuses, including by intelligence and security agencies willing and able to invade the privacy of broad sectors of society – more that is warranted by the threat of terrorism.[22]

Secret, Encrypted, Anonymous and Similar Communications (IAT2)

In order to avoid the use of codes, as in internet Abuse Type 1 (IAT1), and to achieve a much higher general level of security in communications, terrorists and terrorist groups use various methods of secret, encrypting or anonymized communications:

- Secret communications – use of internet capabilities or internet-based software in order to communicate outside of indexed channels, thus avoiding detection and monitoring. One relatively common form is the use of a Virtual Private Network (VPN) - a type of programming that creates a safe and encrypted connection over a less secure network such as the public internet. VPNs operate through the use of shared public infrastructure, while maintaining privacy through security procedures and tunneling protocols whereby the original IP address is exchanged for another, frequently changing, one.
- Encrypted communications – as mentioned in the case of VPN, there are numerous ways and applications that enable communication encryption in some form and with different levels of encryption. Encryption can be applied for voice & video communication (e.g., by scrambling messages) as well as other modes of distant interaction. Encryption software can be easily found and downloaded from the internet.
- Anonymous communications – utilization of internet capabilities to mask the source, location or other parameters of communication which could reveal the identity of persons involved in it. In this case terrorists assume that even if someone monitors the communication, the intercepted information is generally useless since it cannot be linked to specific individuals or terrorist groups. A major drawback of this type of communication is that no names, locations, dates or similar information can appear in

the communication since that may provide clues for revealing the identity of one or more participants in the communication.

Terrorists use various techniques to pass codes for unlocking some forms of communications. In some cases, though, some older and/or simpler methods can be used. Steganography, or the practice of leaving a message hidden in the pixels of pictures, is often overlooked. Such messaging might come in the form of using a predetermined but innocuous code word to send a message or obliquely referencing some shared experience to authenticate true sender identity online.[23] A simple online email account may be used by terrorists for electronic, or virtual, "dead dropping" of communications. This refers to the creation of a draft message, which remains unsent, and therefore leaves a minimal electronic footprint, but which may be accessed from any internet terminal worldwide by multiple individuals with the appropriate password.[24]

IAT2 can be used for all subgroups, providing that clandestine communication form is operational and available to all insider participants in the communication process. However, for financing (SG2) and training (SG3) this type has limited usability – mainly for organizational and consulting segments within the core SG2 & SG3 activities. IAT2 is used for active recruitment, as part of SG1.

Perhaps the easiest way to cope with the (ab-) use of the internet for terrorist plotting within the IAT2 type is to ban and/or restrict the use of clandestine communication techniques for known terrorists or their allies and collaborators. Yet this is easier said than done. Other alternatives might include the use of specialized software for decoding encrypted communications or decrypting them with the assistance of collaborative internet service providers. However, decoding generally requires massive computer power, so again it would be practical to conduct an investigation and restrict decoding and/or decrypting to key suspects in connection with terrorist activities. Furthermore, by tracking the activities of key terrorist suspects it would be possible to spot also steganography, email as well as other forms of anonymous communications.

Brian Fishman, a terrorism expert working for Facebook, suggested a list of questions that technology companies face: How do you determine who is a terrorist? How do you come up with basic content standards? Should companies allow some content from terrorist groups on their platforms in specific circumstances — for instance, in the form of political campaigning by groups like Hezbollah in Lebanon or the Milli Muslim League in Pakistan? : Should some terrorists be completely banned from the platforms no matter what? Should a prohibition extend only to leaders of a terrorist organization or to all known members? How should those categories be defined and what is the evidentiary standard for determining whether someone falls under a category? Moreover, even in the best of circumstances, a company will not be able to create a comprehensive list of the world's terrorists and enforce their exclusion from the internet. Despite this wider problem, establishing stringent restrictions at the user-level can offer a consistent basis for removing terrorist users from a given platform if the internet company provider becomes aware of them.[25] Yet as long as it is possible to open an account on social media without full proof of identity access to the internet for terrorists cannot be effectively banned.

VPN supplies users with a private internet connection in the sense that the traceable personal IP address of the user is replaced with an alternative IP address from a VPN provider. The result is that the user becomes anonymous in practice during the use of the internet, hidden behind the provider's IP address. This makes the identification of terrorists as users difficult. Consequently, it is also more difficult to decide in which cases one should initiate a procedure to block or ban a specific use of VPN. Furthermore, activities combating the (ab-) use of the internet by terrorists in this segment concentrates on individual uses of VPN and not on the technology itself, which remains readily available. While there exist certain methods for VPN

blocking, the terms of use of VPN services have not yet been standardized internationally to make this possible across the board.

Multimedia Materials (IAT3)

Multimedia materials are placed on the internet with the main goal of propaganda; e.g., advertising terrorists and terrorist groups, disseminating their causes and beliefs, in order to attract new followers and reinforce the determination of existing supporters. Such materials range from simple published messages and texts to music or other files uploaded on various dedicated websites. In addition to video streaming from files, there exists also the capability to broadcast live stream video from a mobile phone, tablet or head-mounted camera. Due to possibilities that terrorist components could be recognized in multimedia materials, often resulting in blocking the access to it or other countermeasures, links to multimedia materials can also be sent directly to specific parties. The main difference with simple communications is that multimedia materials often exist also in multiple languages and can be (re-)used by anyone at any time, thus providing potential access to a broad audience with the aim of audience indoctrination for ideological or other goals. At the same time there is no need for terrorists to be directly involved in the process, unless it is a live broadcast of an ongoing attack.

Multimedia materials can also be used for another purpose – psychological manipulation. In that case, the target is the public at large, with the idea of spreading anxiety and fear, which could enhance the effect of terrorist actions, as well as diminish social cohesion. In those cases, multimedia materials often contain scenes of violence (real or fabricated), in combination with insinuations or subtle suggestions intended to spread disinformation. As a secondary effect it is expected that the initial viewers will spread such rumors and provide further publicity for such materials.

Instructional material available online includes tools to facilitate counter-intelligence and hacking activities and to improve the security of illicit communications and online activity through the use of anonymizing techniques. The interactive nature of internet platforms allows the building of a sense of community among individuals from different geographical locations and backgrounds, encouraging the creation of networks for the exchange of instructional and tactical materials.[26] IAT3 can be efficiently utilized mainly for subgroups SG1, SG2 and SG3. For instance, as part of SG1, passive recruitment occurs when terrorist organizations recruit individuals through indirect means, such as addressing groups of people through media campaigns and recruitment materials with the intention of familiarizing them with the aims and activities of the terrorist organization.[27]

Driven by business, user and government prerogatives, major technology and social media companies are investing significant resources into developing measures to respond to terrorist use of their products and services. These efforts are largely approached from a content management perspective and include:

- Adapting terms of service (TOS) and community guidelines to prohibit certain content, activity and forms of behavior. In general, most major internet companies have a zero-tolerance policy for terrorist content and activity on their platforms and have committed themselves to ensuring the safety of their users. In light of the challenges in determining who terrorist actors actually are, some companies use international, regional or national sanctions lists to guide their policies on this issue.
- Developing guidance and systems (human and automated) for content flagging, referral and content/ account removal and for remedial action.
- Establishing guidance and systems for responding to law enforcement and government content/ account removal or data access requests.
- Establishing transparency measures for government requests.
- Establishing, training and sustaining content policy and legal teams.

- Cooperating with government or regional Internet Referral Units (IRUs), when required.
- Developing tools and mechanisms (both human and automated) to counter the narratives of terrorist and violent extremist groups and their followers, carried out in conjunction with government agencies and/ or civil society and community organizations.[28]

As mentioned before, artificial intelligence, machine learning and big data allow some degree of control of multimedia materials on the internet. Identified content that is related to terrorism and terrorist activities can lead to removal and subsequent ban of related multimedia materials. It is known that terrorists use code words to avoid immediate detection, but artificial intelligence and machine learning provide their opponents with the ability to perform in-depth content analysis which can overcome masking attempts. However, there are several potential obstacles for the efficient application of such technologies. The first one is the legal aspect: can such activities be made mandatory to internet providers, or should it be left to private companies to decide when and how to act, in particular in cases when the content in question is ambiguous?

YouTube has a policy for "borderline" content that technically does not violate the company's terms of service: the content can stay online, but it is demonetized (i.e., not linked to advertisements) and not recommended to viewers.[29] Other potential obstacles for application of state-of-the-art technologies are costs considerations for the internet providers themselves.

Dedicated internet Tools (IAT4)

Dedicated internet tools; e.g., interactive websites, chat-rooms, forums, etc. Though slightly outdated and replaced in many cases by social networking platforms, standard internet tools remain in use due to limited security. Internet users can create a website and declare its purpose (true or false) without the need to present any positive identification. The (ab-) use of IAT4 type on the internet for terrorist plotting often involves some level of access restriction such as password protected websites, restricted access to chat-rooms, etc. In cases where websites operate like online stores (e-commerce), selling various items to supporters like books, such websites have to include some form of online payment instrument - which places these in type IAT7.

It is important to distinguish the role of charitable front organizations in IAT4 from their role in IAT7. In IAT4, charities are analyzed regarding their organizational form; i.e., as shells that utilize certain mechanisms to connect and motivate people to get involved in specific activities aiming to achieve predefined goals. Within those activities, more or less openly and on a case-by-case basis, persons are approached with ideological propaganda or radicalizing concepts which can lead to terrorism. The aim is to create bonds with participants in charitable organizations, to get to know them and gain their trust, in order to convert them to become followers. IAT7 type is dealing with the more specific role of charities and certain non-governmental organizations in fundraising. IAT4 is mainly used for subgroups SG1, SG2 and SG3.

Measures used for IAT4 type are based on similar methodologies, software and algorithms as for IAT3, but with a greater focus and finer optimization for web-based contextual searches.

Social Networking Platforms (IAT5)

Social networking platforms differ from other internet tools in the sense that they connect the user (individuals, institutions or other entities), often represented by the user's profile, to other

individuals or groups with the goal of inducing them to exchange opinions, views and all types of information commonly found in social gatherings. The (ab-) use of social networking platforms on the internet for terrorist plotting is usually tolerated by references to the right of freedom of speech, and thus the right to present alternative viewpoints. However, it constitutes an abuse of the freedom of expression to spread violence-oriented propaganda. Unfortunately, there is a broad grey zone existing between two completely opposite issues: the peaceful exchange of ideas, and the glorification of violence. Admittedly, it is not always easy to conclude with certainty whether some online discussion is simply conversation, and when it is hateful propaganda. Furthermore, to block, ban or shut down some specific communication on social networking platforms often requires that some legal procedures have to be initiated which requires that malicious intent has to be proven.

Social networking platforms can also be used for psychological manipulation, as mentioned under IAT3. Social platforms are particularly useful for terrorists for finding potential recruits among vulnerable members of certain social groups. In the case of IAT5, the capability to exchange information and views through social networks offers a framework for the distribution of (dis-) information for terrorists. The objectives are similar with IST3: the creation of anxiety and fear, the undermining of social cohesion and the spreading of false rumors. IAT5 is mainly used for subgroups SG1, SG3 and SG4, although it can also be useful for terrorists during the preparatory phases of attacks (SG5).

Most advanced techniques for detecting terrorist related materials within social networking platforms involve entity recognition and state-of-the-art text analytics in a large body of social media content. Mathematical models together with adequate metaheuristic methods have been designed to provide efficient search mechanisms in social networks with large numbers of users. The designed models and metaheuristics can be used as additional big data analytic tool as follows: they may be combined with existing software for collecting data from the web or for use in already existing professional databases, or they can be used in combination with existing clustering and data mining techniques to improve search quality. There exist also context search algorithms that allow analysis of coverage in multiple languages. However, despite the application of machine learning, fully automatic running of such tools still requires improvements in existing software.

Undoubtedly, some practices - notably restricting content, account removal, providing access to user data for government agencies, or engaging in online social engineering practices - continue to raise important ethical and legal issues.[30]

The question whether or not governments should require tech companies to conduct counter-terrorism operations is politically charged. However, the voluntary efforts made by some of the major internet companies are likely to have a far greater impact on addressing the problem of terrorist exploitation of the internet. For example, in the first nine months of 2018, Facebook removed 14.3 million pieces of content related to the Islamic State, al-Qaeda, and their affiliates, only 41,000 of these items were flagged by external sources, primarily regular users. The overwhelming majority of the content removed was the result of Facebook's voluntary internal efforts.[31]

By raising the awareness of people, it is possible to improve the reporting of offensive content which is terrorism- or extremism-oriented. Early reporting by users of social networking platforms, despite the advances in automatic detection procedures, continues to be an effective way to reduce terrorist (ab-) use of this segment of the internet. In turn, experiences gained from the analysis of user's reporting can be used to improve the operation of automatic detection algorithms and contribute to faster takedown responses.

Online discussions provide an opportunity to present opposing viewpoints or to engage in constructive debate, which may have the effect of discouraging some potential supporters. Counter-narratives with a strong factual foundation may be conveyed through online discussion forums, images and videos. Successful messages may also demonstrate empathy

with the underlying issues that contribute to radicalization, such as dire political and social conditions, and highlight alternatives to violent means of achieving desired outcomes. Strategic communications that provide counter-narratives to terrorist propaganda may also be disseminated via the internet in multiple languages, to reach a broad, geographically diverse audience.[32]

Social media platforms often define terrorism and extremism in their own way. Facebook's original definition of terrorism, for example, was "any non-governmental organization that engages in premeditated acts of violence against persons or property to intimidate civilian, population, government, or international organization in order to achieve a political, religious, or ideological aim."[33] This definition was subsequently modified to focus its application to terrorist organizations. However, we know that terrorist groups often draw on ideas developed by extremist organizations. Extremism – both violent and non-violent – can lead to terrorism.

Therefore, to stop social media platforms being used by extremists and terrorists, technology companies might wish to take the following steps. First, they should create new "extremism" or "terrorism" categories within their existing reporting systems. This would allow users of their platforms – including the public, or people known to terrorists who are concerned about the material shared with them – to report and flag such materials. On YouTube, users can flag a video uploaded by a member of the public as "violent or repulsive" or as "promoting terrorism" or as "hateful or abusive content," but not all three. The overlapping nature of this material needs to be acknowledged by allowing multiple flags. Second, a better and more consistent appeal process and feedback mechanism should be created. This is particularly important for material that is not taken down from these platforms. Users should be able to have a conversation with decision makers, and decisions should be explained thoroughly and transparently, breaking down why some material is allowed to remain on the platform, and other online material is removed. While some companies publish quarterly reports or blog posts on this issue, we need to move beyond metrics to specific case studies and aim for more open conversations between consumers and social media companies.[34] Good examples of reports that provide relevant information on tools and policies are "Hard Questions: What Are We Doing to Stay Ahead of Terrorists?"[35] and "Combating Hate and Extremism" – both by Facebook.[36]

In many countries, recruitment into terrorist organizations occurs not only through direct social contacts but also on online platforms. Regarding the latter: one opportunity for operational intelligence and security agencies is to work more closely with social media and internet and web-hosting providers. Where content promoting terrorism or facilitating recruitment activities is found, financial investigations should be initiated to determine who controls and finances suspect accounts. While in some cases no financing may be involved, some of the case studies indicate that professionals have been hired to develop a platform to spread terrorist material.[37]

Video Games and Similar Interactive Means of Promotion (IAT6)

This type of (ab-) use of internet activities is related to interactive means of promotion, downloadable from the internet. Providers range from file-sharing sites to cloud repositories. The difference with dedicated internet tools (IAT4) is that IAT6 assumes that interactive promotion is only delivered (downloaded) over the internet and subsequently used offline or as a local installation with an internet connection. Typical examples would be video games (which can also be used for training purposes), interactive learning systems, magazines and brochures in digital form for downloading and offline browsing. These are often are available in multiple languages to increase audiences and impact. IAT6 is very difficult to combat since the downloaded promotion materials are no longer "visible" on the internet. Therefore, even when some content is banned or blocked at a specific web location, it can still circulate by

direct coping or reappear at new locations, possibly published by another terrorist member, supporter or sympathizer who has downloaded it in the first instance.

Some uses of the internet and of internet communication technologies (ICT) for terrorist purposes are often indistinguishable from regular use of the internet by ordinary users or groups, making it very difficult to address the issue. Calls by governments at the international, regional and national levels to take "urgent action" against online extremism or terrorist use of the internet are growing, notably in terms of restricting online content with the aim of protecting public safety. Such calls to action tend to be directed against intermediaries (i.e., internet service providers, technology enterprises and social media companies) rather than the actual creators of the content. This is often due to the fact that creators of terrorist content operate out of foreign jurisdictions or places, where law enforcement is weak. There are competing arguments as to the merits of various approaches. On the one hand, these are often perceived as enhancing public safety and protecting the vulnerable. On the other, some hold that interventions violate the human rights of users, and undermine trust in companies as well as in government. In short, much needs to be done by all parties to ensure a more appropriate balance between offline prevention and online counter measures and in demonstrating convincingly what methods yields effective results.[38]

It is important to emphasize the distinction between mere propaganda and material intended to incite acts of terrorism. In some national jurisdictions, in order to be held liable for incitement to terrorism, a showing of the requisite intent and a direct causal link between alleged propaganda and an actual plot or execution of a terrorist act is required. For example, in a contribution to an expert group meeting, a French expert indicated that the dissemination of instructive materials on explosives would not be considered a violation of French law unless the communication contained information specifying that the material was shared in furtherance of a terrorist purpose.[39]

Online Payment Tools (IAT7)

In contrast to simple and low-cost approaches to general online recruitment, referred to above, terrorist organizations are often spending considerable amounts of money on recruitment networks and on expenses related to gathering and "processing" recruits. Quite often new recruits have to move to specific locations (requiring fake identities, travel and accommodation expenses), and in such cases there is also often remuneration involved (not unlike payments to mercenaries). Recruitment networks frequently use premises of registered or unregistered religious organizations, places of worship or similar locations as assembly points. Sometimes premises have to be rented. Even more expenses have to be incurred for the preparation and execution of terrorist acts. In order to finance all this, terrorist organizations have to collect and transfer amounts of money to specific locations.

Online payment systems are basically used for transfer of funds from different sources to accounts belonging to, or handled by, terrorist organizations (e.g., in the case of shell companies) or funds are transferred to designated individuals (frequent using false or masked identities). Funds might have various origins, starting from direct solicitation, illegal businesses and money laundering, through transfer of cash collected by hand by associates. Yet, funds can also be obtained from legal business or might include legitimate donations. There are also possibilities of engaging hackers, belonging to, or associated with terrorists, to perform phishing, hacking or similar activities that involve transfer of stolen money to terrorists' accounts. In general, the internet offers a number of advantages that are of interest to terrorists. To mention just a few: global coverage and reach, technological advance in commerce on the international level with commonly accepted ways of handling electronic transfers of funds (including online banking, mobile phone banking, etc.) and the use of legitimate ways to collect money for terrorist needs (e.g., gambling, crowd-sourcing, e-

commerce, virtual sales, etc.). In contrast to online criminal activities involving terrorists, which are the target of international police investigations on a daily basis, the activities of charities and nongovernmental organizations (NGOs) are much more problematic to control. It is very difficult to distinguish charities and NGOs with legitimate goals from those which are meant to finance acts of terrorism, in particular when the cause is masked with false pretenses, or when charities and NGO are infiltrated by terrorists who deflect part of the income for their own nefarious purposes.

In the Eurasian region, recruitment often occurs through religious organizations and in a number of cases the majority of the members of terrorist organizations are recruited by established recruitment networks which require financial support. In addition, maintaining a digital magazine and keeping IT teams engaged requires a continuous funding stream. Although the access and use of social networks and the creation of websites is low-cost and can even be free of charge, some terrorist organizations create high-quality content, which tends to require the involvement of experts and the use of sophisticated equipment. Due to the scale and variety of forms of distribution of this type of content, it is likely that a number of bloggers and moderators are participating in the distribution of the material. There are opportunities for strengthened co-operation between the key operational authorities within national counterterrorism/counter-financing of terrorism (CT/CFT) frameworks, particularly the units in charge of terrorist financing investigations and those involved in the collection of intelligence data on recruiting activities. Often, these functions are performed by different investigative entities which operate in separate spheres which can make the detection of recruitment financing activities more challenging. CT-professional should take note of FATF's (Financial Action Task Force) work on interagency CT/CFT information sharing which offers good practices as well as practical tools.[40] IAT7 can be efficiently utilized mainly for subgroups SG2 and SG5.

There is widespread agreement at this point among governments that the internet has created serious counterterrorism vulnerabilities and that action is needed to counter this growing threat. There is far less agreement, however, on what concrete steps can and need to be taken. The US government has taken a number of unilateral aggressive actions in this area, specifically designed to address the abuse of the internet for terrorist financing purposes. This has included a number of prosecutions of suspected terrorists for their internet-related activities. The US has also used its law enforcement tools more broadly, targeting money remitters without adequate internal anti-money laundering/counter terrorist financing compliance systems. Not all countries have been as proactive as the US on this front. First, many countries lack the technical capabilities necessary to investigate online terrorist activity. Second, there is still a debate about how far governments should go in cracking down on some internet-related activities. Some governments are concerned that taking drastic steps will curtail the right to freedom of expression. There is also an active debate about what works best from a counterterrorism perspective – particularly whether it is more valuable to monitor terrorists' activities on the internet for intelligence purposes, or to shut their websites down. Third, the laws in this area have not kept up with the technological changes, and there is no international agreement about what changes should be made to move forward. Some of the actions of the United States are a step in the right direction, but without broader international cooperation on this issue, there are limits to what can be accomplished.[41]

Exploitation of Publicly Available Information & Resources (IAT8)

This type of (ab-) used internet activities is covering a very broad area. Therefore, it is quite difficult to provide extensive coverage of all possible cases. Some examples might include Google, Instagram, Facebook, Wikipedia, etc. – in essence any public internet source that provides information useful for specific terrorist purposes and objectives.

Organizations and individuals often publish large amounts of information on the internet. In the case of organizations, this may be a result of a desire to promote their activities and encourage interactions with customers and the public in general. Some sensitive information that may be used by terrorists for illicit purposes is also made available through internet search engines, which may catalogue and retrieve inadequately protected information from millions of websites. Furthermore, online access to detailed logistical information, such as real-time closed-circuit television footage (CCTV), and applications such as Google Earth, which is intended for, and primarily used by, the public for legitimate ends, may be misused by those intent on benefiting from the free access to high-resolution satellite imagery, maps and information on terrain and buildings for the reconnaissance of potential targets from a remote computer terminal.[42]

Particular risks may ensue when terrorists gather information related to critical infrastructures, which allow them to discover vulnerabilities and facilitate more precise targeting. Ranging from airports and other transportation related infrastructure to power- and water- supply systems which are vital for society (including nuclear power plants), serious damage to critical infrastructure can result in both direct and indirect damage, including loss of lives. For this reason, the segments of the (ab-) use of the internet for terrorist plotting and related purposes that overlap with Critical Infrastructure Protection (CIP) and resilience activities should be merged and handled as a coordinated activity.[43]

Militants use online mapping tools to plan attacks, monitor news, and identify potential recruits. Various platforms can be used for these purposes, including social media, traditional media, search engines, and specialized tools for identifying sensitive targets. These are the same tools that are used by ordinary folks to find grocery stores, reconnect to old friends, and search for the quickest ways to get from A to B.[44] However, in fact these are also dual use tools that can be abused by terrorists.

IAT8 is mainly used for subgroups SG4 (e.g., intelligence gathering) and SG5, with emphasis on the latter. Due to the abundance of information on the internet, IAT8 might also be used for other subgroups, depending on the specific terrorist's plans and goals.

Unfortunately, this type of instrument requires the most painstaking efforts to counteract. There is no tool on the internet for direct analysis and recognition, either by humans or by automated systems that can tell when open sources are used for good or evil. Only by following globally the activities of terrorists and their supporters on the internet might it become possible to guess with some degree of confidence their motivation and target selection. The effectiveness of such actions would have to be based on several assumptions: that the terrorists are known, that their web-based activities are monitored, that it is possible to find a behavioral pattern within their internet searches that can indicate specific terrorist aims and, finally, that there is enough evidence for taking preemptive legal or operational action.

It would be much more productive to conduct surveillance of web-based activities of known or suspected terrorists once there are indicators of terrorist plotting from other IAT categories. In that case such indicators could identify behavioral patterns that could guide the search for the proverbial needle in the haystack. However, the issue of use of gathered data as evidence in court for any legal action remains to be solved.

Cyberattacks (IAT9)

Cyberattacks represent a category of its own, since the impact and expansion of such attacks are related to the general growth of cyber systems. The preparation for cyberattacks involves various other, already discussed above, internet activities like communication, propaganda, fund raising, recruitment, etc. (i.e., from SG1 to SG5). Therefore, cyberattacks are mentioned here for reference purposes only, because strictly speaking as a type they are also part of internet activities (ab-) used by terrorists.

In recent years, there has come into existence a whole new discipline named Cyber Protection. It studies cyberattacks and designs counter-measures. Due to the complexity of the problem, to prevent and combat cyberattacks, cyber protection requires a range of national and cross-border efforts.

There is an urgent need to develop an international game plan in order to combat cyberattacks by terrorists. To this end, an 8-step global counter cyber-terrorism game plan has been proposed:[45]

- **Step 1**: Reaching a common definition of terrorism and cyber terrorism is the starting point. Which activities on the internet (e.g., hacking, propaganda, attacking to infrastructures etc.) should be counted as cyber terrorism must be defined exactly. Speaking the same language and creating a common technical language should be the starting point.
- **Step 2**: Essential national and international legal measures have to be taken. International legal arrangements must be put in place. Accordingly, national legislation has to be harmonized with international treaty obligations.
- **Step 3**: Both bilateral and multilateral agreements on cyber security cooperation must be signed, ratified and implemented between countries.
- **Step 4**: An intelligence pool (e.g., in the form of fusion centers) needs be created in order to collect and share intelligence simultaneously in real time between participating countries. Collecting intelligence should include not only monitoring terrorist websites but also collecting electronic evidence about plots to engage in cyberattacks.
- **Step 5**: Cyber defense expert teams ought to be created and put in charge to act internationally whenever a country encounters a cyberattack. The number of quick national response teams ought to be increased, e.g., with the help of NATO's Computer Incident Response Capability and the Estonia-based Cooperative Cyber Defense Centre of Excellence. An international cyberattack response training program should be established.
- **Step 6**: International counter-cyberattack exercises should be planned and executed in order to help participating governments to demonstrate and share their proficiency and experience.
- **Step 7**: A well-organized international decision-making process that spans from detection to neutralization (or disruption) of cyberattacks should be formed. Internationally authorized executives should respond to any attack affecting international security, based on pre-agreed rules of engagement.
- **Step 8**: After-reaction analyses should be conducted in order to identify and improve weaknesses in the defense process. A feedback, 'lessons learned' mechanism should be put in place in order to improve reaction for the next attack.

Conclusion

Preventing terrorists from (ab-)using the internet is in many ways a Sisyphean task. The more the society and specialized agencies develop and apply measures to counteract terrorists, the more terrorists are likely to adapt and find new ways to exploit the internet for their purposes. However, the situation is not hopeless, and one should not reduce efforts to counter abuse. One should not be intimidated into accepting the continued existence of terrorism and its expansion online which, at least in part, is due to the mixed blessings of the internet.

This chapter systematic analysis of uses and abuses of the internet for terrorist plotting and related purposes can serve as a good starting point for non-experts to understand the basic tools and methods that terrorists use. That should help to enhance the capability of governments and

societies to react to terrorist propaganda. With greater public awareness of terrorists' online activities, attentive ordinary users of the internet can, in fact, become part of an early warning system for the prevention of internet abuse by extremists and terrorists.

The analyzed prevention methods and the counter-measures suggested against the (ab-) use of the internet for terrorist plotting and related purposes should also be of use for professionals who are involved in counter-terrorism. While experts on terrorism from law enforcement and from intelligence agencies certainly know more details about terrorists' modus operandi, they often lack a hands-on experience on how IT providers operate on day-to-day basis. On the other hand, web service providers, websites hosts and other specialized private IT sector stakeholders are usually more focused on general continuity of service issues than on possible terrorist abuse of their instruments and technologies. As has been emphasized repeatedly in this chapter, there is a need for close cooperation and improved public-private partnerships between all state and civil society stakeholders when it comes to preventing the mis- and abuse of the world wide web and the internet. As creators of the new system for the categorization of (ab-) uses of the internet for terrorist plotting presented in the preceding pages, we hope that this classification will assist others in more effectively combating terrorist (ab-) uses of the internet.

Dr. Branislav Todorovic is a member of the Institute for National and International Security (INIS), Serbia, and a Senior Research Associate in NTUA – National Technical University of Athens and AUA – Agricultural University of Athens, Greece. He also cooperates since 1989 with MASBG – Faculty of Mechanical Engineering, University of Belgrade, Serbia. He is a full member of the Technical Chamber of Greece (TEE) and the Technical Chamber of Serbia. Branislav Todorovic has participated in many commercial and R&D projects, and produced international conference papers. His background covers 30 years of work in environmental sciences, energy and water topics, Critical Infrastructure Protection (CIP), cyber security and IT/ICT, especially GIS, CAD, programming & software development, 3D modelling, databases, etc. He has worked in multidisciplinary projects related to capacity building, public participation, energy and water resources management, renewable resources, modelling of processes, Decision Support Systems (DSS), expert systems, and complex designs.

Dr. Darko Trifunovic is a Senior Research Fellow and lecturer at the Faculty of Security Studies of the University of Belgrade and a Senior Adviser at the Research Institute for European and American Studies in Athens, Greece. He is also a guest professor at FUDAN University – Center of American Studies, Shanghai, China. Dr. Trifunovic is a specialist in Security Studies, Intelligence & Counter Intelligence Studies as well as Counter-Terrorism, National and International Security Studies. He is a former diplomat (First Secretary of the Foreign Service of BiH at the UN). Dr. Trifunovic is the representative for Serbia and Montenegro in the International Strategic Studies Association (ISSA). He is a member of the Advisory Board of the Institute of Transnational Studies, Munich, Germany. Dr Trifunovic is regular speaker at the International Counter Terrorism Institute, Tel Aviv, Israel, and one of the founding Members of the International Counter Terrorism Academic Community (ICTAC). He has published a number of academic books, papers and articles.

Endnotes

[1] See more: Trifunovic, Darko, *Cyber Security-Virtual Space as an area for covert terrorist activities of radical Islamism.* Nis: Teme, 2019.
[2] Cf. Cambridge University Press, official website; Available at: https://dictionary.cambridge.org/
[3] A secondary critical issue in relation to this topic, is the possible misuse of the information presented in the following pages. However, this chapter will present mainly publicly known methods for the prevention of the (ab-) use of the internet by terrorists. It is up to the professional CT reader, in case there is a need, to get in touch with institutions or projects dealing actively with the issue under consideration for more detailed and operational useful information.
[4] Andrew Glazzard, "Shooting the Messenger: Do Not Blame the Internet for Terrorism," *RUSI Newsbrief*, 15 February 2019.
[5] Idem.
[6] UNODC, *The Use of the Internet for Terrorist Purposes*. Vienna: United Nations Office on Drugs and Crime, 2012, pp. 3-26.
[7] United Nations. *Countering the Use of the Internet for Terrorist Purposes — Legal and Technical Aspects*, New York: United Nations Counter-Terrorism Implementation Task Force, (Working Group Compendium May 2011), This is a shortened version of a report; for full version, see: www.un.org/en/terrorism/ctitf/wg_counteringinternet.shtml,
[8] Coninsx, Michèle, 'Responding to terrorist use of the internet' (2019), Global Initiative, p. 1; Available at: https://globalinitiative.net/terrorist_use_internet/ .
[9] See, for example, International Covenant on Civil and Political Rights (General Assembly resolution 2200 A
(XXI), annex), art. 19, para. 2.
[10] UNODC, *The Use of the Internet for Terrorist Purposes*. Vienna: United Nations Office on Drugs and Crime, 2012. Available at: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.
[11] Gerwehr, Scott and Daly, Sarah 'Al-Qaida: terrorist selection and recruitment', in: David Kamien (ed.) *The McGraw-Hill Homeland Security Handbook*. New York, McGraw-Hill, 2006, p. 83.
[12] Denning, Dorothy E., 'Terror's web: how the internet is transforming terrorism'; in: Yvonne Jewkes and Majid Yar Cullompton (eds.) *Handbook of Internet Crime*, edited by, UK, Willan Publishing, (2010, pp. 194-213.
[13] Weimann, Gabriel, 'Online terrorists prey on the vulnerable', *Yale Global Online*, 5 March 2008; Available at: www.yaleglobal.yale.edu/content/online-terrorists-prey-vulnerable.
[14] Office of the United Nations High Commissioner for Human Rights, "Human rights, terrorism and counterterrorism," Fact Sheet No. 32 (Geneva: UNHCR, 2008), Chap. III, sect. H.
[15] Conway, Maura, "Terrorist 'use' of the internet and fighting back," *Information & Security*, Vol. 19 (2006), pp. 12-14.
[16] Cf. Trifunović, Darko, 'Islamic Terrorism and al-Qaeda in the Balkans (Testimony of a former al-Qaeda lieutenant)', International Strategic Studies Association, Alexandria, VA.: ISSA, 2014 and UN report referred to in note 10.
[17] Trifunović, Darko, *Digital steganography in terrorist networks*, SYM-OP-IS 2015: XLII International Symposium on Operations Research, 2015, Vol. V(1).
[18] Pursuant to the International Telecommunication Union Toolkit for Cybercrime Legislation, section 1 *(n)*, malware may be defined as a program that is inserted into a computer program or system, usually covertly, with the intent of compromising the confidentiality, integrity or availability of the computer program, data or system.

[19] Kavanagh, Camino et al, 'Private Sector Engagement in Responding to the Use of the internet and ICT for Terrorist Purposes - Strengthening Dialogue and Building Trust', ICT4Peace Foundation and UNCTED, 2016.
[20] INTERPOL, *Southeast Asia: Countering terrorist use of the Internet*, Report from Vietnam, 2018; Available at: https://www.interpol.int/en/News-and-Events/News/2018/Southeast-Asia-Countering-terrorist-use-of-the-internet
[21] Fishman, Brian, *Crossroads: Counter-Terrorism and the internet*, *Texas National Security Review*: Volume 2, Issue 2 (February 2019), pp. 83-100.
[22] Coninsx, Michele, op. cit.
[23] Fishman, Brian, op. cit., p. 86
[24] UNODC (2012) , op. cit., p. 10
[25] Owen, Laura H., 'Terrorists use the internet in much the same way as other people." How should tech companies deal with it?' *NiemanLab*, Cambridge, Mass.: Nieman Foundation (Harvard) (2019) Available at: https://www.niemanlab.org/2019/04/terrorists-use-the-internet-in-much-the-same-way-as-other-people-how-should-tech-companies-deal-with-it/ .
[26] UNODC (2012), op. cit. p. 8
[27] FATF, Financing of Recruitment for Terrorist Purposes, FATF, Paris (2018); URF: www.fatf-gafi.org/publications/methodsandtrends/documents/financing-recruitment-terrorist-purposes.html
[28] Kavanagh, Camino et al, op. cit., p. 5.
[29] Owen, Laura H., op. cit.
[30] Kavanagh, Camino et al, op. cit., p. 6.
[31] Fishman, Brian, op. cit., p.83.
[32] UNODC (2012), op. cit.
[33] Facebook, *Community Standards, Part 2: Dangerous Individuals and Organizations*, 2020; Available at: https://www.facebook.com/communitystandards/dangerous_individuals_organizations
[34] Malik, Nikita, *The Fight Against Terrorism Online: Here's The Verdict*, Cybersecurity, Forbes (2018) Available at: https://www.forbes.com/sites/nikitamalik/2018/09/20/the-fight-against-terrorism-online-heres-the-verdict/#70a0cf814dc5
[35] Bickert, Monika and Fishman, Brian, *Hard Questions: What Are We Doing to Stay Ahead of Terrorists?*, Facebook Hard Questions series, 2018; Available at: https://about.fb.com/news/2018/11/staying-ahead-of-terrorists/
[36] Facebook, *Combating Hate and Extremism*, 2019; Available at: https://about.fb.com/news/2019/09/combating-hate-and-extremism/
[37] FATF, op. cit.
[38] Kavanagh, Camino et al, op. cit. p.5
[39] UNODC (2012), op. cit.
[40] FATF, op. cit.p.25.
[41] Jacobson, Michael, "Terrorist Financing on the Internet," *CTC Sentinel*, Vol.2, Issue 6, June 2019.
[42] UNODC (2012), op. cit.
[43] See for more on this: Todorovic, Branislav et al, *Chapter 22 - Contribution to Enhancement of Critical Infrastructure Resilience in Serbia, Resilience and Risk - Methods and Application in Environment, Cyber and Social Domains*, Proceedings of the NATO Advanced Research Workshop on Resilience-Based Approaches to Critical Infrastructure Safeguarding, Azores, Portugal, 26–29 June 2016, pp 531-551.
[44] Fishman, Brian, op. cit.
[45] Based on Dogrul, Murat, Aslan, Adil and Celik, Eyyup, *Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism*, 2011 3rd International Conference on Cyber Conflict, Tallinn, Estonia (2011), pp 29-43.

Bibliography

Braham, M. and Droogenbroeck, M.V. *Deep background subtraction with scene-specific convolutional neural networks*, International Conference on Systems, Signals and Image Processing (IWSSIP), 2016.

Cambridge University Press, Official website. Available at: https://dictionary.cambridge.org/

Coninsx, Michèle, 'Responding to terrorist use of the internet' (2019), Global Initiative. Available at: https://globalinitiative.net/terrorist_use_internet/ .

Conway, Maura, 'Terrorist "use" of the internet and fighting back', *Information & Security*, Vol. 19 (2006), pp. 12-14.

Denning, Dorothy E., 'Terror's web: how the internet is transforming terrorism"; in: *Handbook of internet Crime*, edited by Yvonne Jewkes and Majid Yar. Cullompton, UK, Willan Publishing, (2010)), pp. 194-213.

Dogrul, Murat, Aslan, Adil and Celik, Eyyup. *Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism*. 3rd International Conference on Cyber Conflict, Tallinn, Estonia (2011), pp 29-43.

FATF, Financing of Recruitment for Terrorist Purposes, Paris: FATF, 2018. Available at: www.fatf-gafi.org/publications/methodsandtrends/documents/financing-recruitment-terrorist-purposes.html

Fishman, Brian, 'Crossroads: Counter-Terrorism and the internet', *Texas National Security Review*: Volume 2, Issue 2 (February 2019), pp 83-100.

Gerwehr, Scott and Daly, Sarah, 'Al-Qaida: terrorist selection and recruitment', in *The McGraw-Hill Homeland Security Handbook*, edited by David Kamien. New York, McGraw-Hill, 2006), pp. 73-89.

Glazzard, Andrew. "Shooting the Messenger: Do Not Blame the internet for Terrorism," RUSI Newsbrief, 15 February 2019.

International Covenant on Civil and Political Rights (General Assembly resolution 2200 A (XXI), annex), art. 19, para. 2.

Jacobson, Michael, 'Terrorist Financing on the Internet*', CTC Sentinel*, Vol. 2, Issue 6, June 2019.

Kavanagh, Camino et al, *Private Sector Engagement in Responding to the Use of the internet and ICT for Terrorist Purposes - Strengthening Dialogue and Building Trust*, A project sponsored by the Governments of Spain and Switzerland, and Facebook, Microsoft and Kaspersky Lab: ICT4Peace Foundation and UNCTED, 2016.

Office of the United Nations High Commissioner for Human Rights, 'Human rights, terrorism and counterterrorism', Fact Sheet No. 32 (Geneva: UNHCR, 2008, Chap. III, sect. H.

Redmon, J. and Farhadi, A., *YOLOv3: An Incremental Improvement*, Computer Vision and Pattern Recognition (CVPR), 2018.

St.Charles, P-L., Bilodeau, G-A. and Bergevin, R. *SuBSENSE: A Universal Change Detection Method With Local Adaptive Sensitivity*, IEEE Transactions on Image Processing, (Vol.: 24 (1), 2015.

Todorovic, Branislav et al, *Chapter 22 - Contribution to Enhancement of Critical Infrastructure Resilience in Serbia, Resilience and Risk - Methods and Application in Environment, Cyber and Social Domains*, Proceedings of the NATO Advanced Research Workshop on Resilience-Based Approaches to Critical Infrastructure Safeguarding, ISBN 978-94-024-1122-5 (HB), Azores, Portugal, 26–29 June 2016, pp. 531-551.

Trifunovic, Darko, *Cyber Security-Virtual Space as an area for covert terrorist activities of radical Islamist*. Nis: Teme, 2019.

Trifunović, Darko, *Digital steganography in terrorist networks*, SYM-OP-IS 2015: XLII International Symposium on Operations Research, Vol. V (1), 2015.

Trifunović, Darko, *Islamic Terrorism and al-Qaeda in the Balkans (Testimony of a former al- Qaeda lieutenant)*, International Strategic Studies Association, Alexandria, VA.: ISSA, 2014.

United Nations. Countering the Use of the internet for Terrorist Purposes — Legal and Technical Aspects, United Nations Counter-Terrorism Implementation Task Force, (Working Group Compendium May 2011), This is a shortened version of the report which can be found in full at: www.un.org/en/terrorism/ctitf/wg_counteringinternet.shtml United Nations New York, 2011, pp 9-10

UNODC. *The Use of the internet for Terrorist Purposes*, Vienna, UNODC, 2012, pp. 3-26.

Weimann, Gabriel, 'Online terrorists prey on the vulnerable', YaleGlobal Online, 5 March 2008. Available at: http://yaleglobal.yale.edu/content/online-terrorists-prey-vulnerable.

Web-based Resources

Bickert, Monika and Fishman, Brian, *Hard Questions: What Are We Doing to Stay Ahead of Terrorists?*, Facebook Hard Questions series, 2018; Available at: https://about.fb.com/news/2018/11/staying-ahead-of-terrorists/

Facebook, *Combating Hate and Extremism*, 2019; Available at: https://about.fb.com/news/2019/09/combating-hate-and-extremism/

Facebook, *Community Standards, Part 2: Dangerous Individuals and Organizations*, 2020; Available at: https://www.facebook.com/communitystandards/dangerous_individuals_organizations

INTERPOL, *Southeast Asia: Countering terrorist use of the internet*, Report from Vietnam, 2018. Available at: https://www.interpol.int/en/News-and-Events/News/2018/Southeast-Asia-Countering-terrorist-use-of-the-internet

Malik, Nikita, 'The Fight Against Terrorism Online: Here's The Verdict', *Cybersecurity, Forbes* (2018); Available at: https://www.forbes.com/sites/nikitamalik/2018/09/20/the-fight-against-terrorism-online-heres-the-verdict/#70a0cf814dc5

Owen, Laura H., "Terrorists use the internet in much the same way as other people. How should tech companies deal with it?," NiemanLab, Cambridge, Mass.: Nieman Foundation, Harvard University, (2019); Available at: https://www.niemanlab.org/2019/04/terrorists-use-the-internet-in-much-the-same-way-as-other-people-how-should-tech-companies-deal-with-it/