Organization for Security and
Co-operation in Europe

OSCE Online Expert Forum Series on Terrorist Use of the Internet: Threats, Responses and Potential Future Endeavours

Final Report

Action against Terrorism Unit
Transnational Threats
Department
OSCE Secretariat
Wallnerstrasse, 6
A-1010 Vienna,
http://www.osce.org/atu

Contents

I. Summary

In 2012, the OSCE Secretariat Transnational Threats Department/Action against Terrorism Unit (TNTD/ATU) organized four online expert forum discussions designed to reinvigorate and further stimulate information exchange on the latest trends and debates related to terrorist use of the Internet, pertinent challenges in responding to such threats as well as relevant good practices and policy options.

One key component of this initiative was to elaborate on options on how the OSCE could further complement international efforts in this field building on existing mandates. This has become of particular relevance now that participating States adopted Permanent Council Decision No. 1063 on an OSCE Consolidated Framework for the Fight Against Terrorism (December 2012), which lists countering the use of the Internet for terrorist purposes as a strategic focus area for OSCE counter-terrorism activities.

Overall, 140 experts participated representing national authorities of participating States, civil society organizations, academia and the business community. Experts contributed to discussions with over 164 posts tackling and shedding light on key discourses in this field, offering potential solutions, showcasing national good practices and relevant international initiatives as well as offering their views on areas the OSCE could get more involved by building on its comparative advantages.[1]

II. Key Themes and Recommendations

- **A harmonized international legal framework** is essential to bring cyber terrorists to justice, and a key component of international law enforcement co-operation, not least because a large number of countries base their mutual legal assistance regimes on the principle of “dual criminality”. Internationally compatible, adequate and well thought-through laws are also the best guarantee to ensure both security and privacy but also international co-operation. National legal frameworks need to be regularly reviewed against international developments to take into account the rapid developments in technology.

- **Co-operation at the practitioner level is essential** especially in the absence of a harmonized international legal framework and the rapid developments of Internet technology to ensure the timely response to terrorist use of the Internet. This should include a two speed approach: On the first responder/law enforcement level this should involve fast real-time communication lines, and on the judicial level it should include thorough processes to ensure the usability of evidence in courts. More broadly, countries should also consider establishing relevant focal points as part of their diplomatic missions in order to enhance co-operation. *The OSCE could consider continue*

[1] Contributions by experts do not necessarily reflect the views of the OSCE Secretariat. Although utmost care was taken to reflect all contributions in the report, for the sake of clarity and readability posts had to be summarised in line with key messages and themes!

acting as an information sharing platform for practitioners complementing mechanisms by other international organizations.

- **Efforts to tackle terrorist use of the Internet should be preventive and maintain an open Internet. Any necessary invasive action needs to be narrowly defined.** Controlling all terrorist/criminal online content is unrealistic and it is better to maintain an open Internet rather than shutting down websites. However, at times more invasive measures are indispensable especially if activities cross certain red lines e.g. inciting violence or if imminent danger looms. Such measures including blocking websites or taking down material need to go in parallel with clear cut national laws and international commitments and policies that respect fundamental rights and clearly lay down what threats justify what measures. In addition, it is important to establish an effective system for oversight that provides the opportunity for the affected party to complain if wrongfully targeted. Policies need to involve and solicit the contributions by the public and civil society. This is important in order to demystify what authorities are seeking to achieve and avoid risking a public relations backlash which in turn creates opportunities for terrorists. Likewise, authorities need to be mindful how such efforts impact on international co-operation and on-going investigations in other jurisdictions. *Organizations such as the OSCE can be an ideal place to evaluate potential invasive measures not only in terms of their compatibility with fundamental freedoms but also with regard to evaluating the costs and benefits of such measures.*

- **While data collection can be supported by technology, it is intelligence resulting from the combination of information provided by multiple sources including the public and other services that will provide the most complete picture.** In times of budgetary constraints, trained human resources capable of analysing an ever growing amount of communication data need to be as effective as possible and importantly need to take into account the human factor. While authorities are capable of collecting vast amounts of data, the technical capacity to sift through that data in a meaningful way has not been developed at the same pace, with the result that human intervention and analysis remains indispensable. Such intelligence should identify the main adversary groups and constantly probe and monitor their activities. Easy to use and focused intelligence is therefore key!

- **Effective steps to counter terrorist use of the Internet require strong and mutually beneficial public-private partnerships (PPPs)**. A secure cyberspace is as much in the interest of States as it is for businesses as part of safeguarding financial interests and reputation. The expertise as well as technical knowledge available from the private sector should be sought and utilised in a systematic manner including by formulating clear-cut, unambiguous laws regulating co-operation and mindful of each other’s roles and responsibilities. Such co-operation could also build on co-operation guidelines that are elaborated on jointly and implemented by all stakeholders with a clear commitment to engage long-term. As part of co-operating effectively both sides need to identify focal points empowered to speak on behalf of their outlets. In this regard co-operation within the private sector could also be enhanced by e.g. forming an umbrella organization which allows the private sector to speak with one voice. More debate is needed with regard to businesses’ or indeed user liability pertaining to inadequate cyber/ICT security measures. *Existing private sector contributions or PPPs should be supported such as flagging and reporting mechanisms or co-operation best practices and in this regard organizations such as the OSCE are key in promoting such efforts and public education initiatives*.

- **Internet users are an essential part of countering terrorist use of the Internet.** On the individual level, there is a need for enhanced end user awareness raising on the responsible use of the Internet and possible consequences of careless personal data disclosure. Raising awareness and educating the individual Internet user on how to stay safe should start at the beginning of a child's educational career including e.g. by passing an exam on cyber/ICT security, and continue throughout working life and retirement age. On a group level, mechanisms and frameworks need to be created for Internet users to look after each other. This needs to include adequate reporting/flagging mechanisms by the private and/or public sector and expertise on what to report. Civil Society Organizations (CSOs) have a special role to play in this regard both in terms of countering terrorist narratives and in strengthening end-user resilience as well as reporting of terrorist content. More debate is needed with regard to user liability and how to enlist the help of Internet users in emergency situations. *The OSCE could play a key role in encouraging States to implement such educational programs and offer capacity building assistance in this regard.*

- **More cross-fertilization is needed on efforts combating different forms of (violent) extremism online.** While it is important to recognize and deal with hate crimes and other forms of extreme right wing violence as separate, distinct issues, especially in terms of education, awareness raising, law enforcement and justice agency response, the question of possible overlap between preventing such expressions of violence and preventing terrorism nevertheless arises. For instance more research is needed on the tipping points when extreme views turn violent. This means that some baseline knowledge is made available that can be used to counter all forms of extremism. Such a baseline would be inclusive of all factors, including motivation, to be better prepared for potential future new forms of violent extremism. In this regard it is also important to intensify efforts to compare methods and identify commonalities between different forms of counter measures to tackle different forms of extremism e.g. counter narratives vs. countering xenophobic statements. *The OSCE with its comprehensive approach to security could lead a balanced review by looking into the aforementioned issues.*

III. Background

TNTD/ATU Mandate and Activities

Concerned over the extent of the use of the Internet by terrorist organizations, OSCE participating States (pS) adopted two Ministerial Council Decisions that serve as the basis for the TNTD/ATU's on-going active role in this area. Specifically, participating States committed to exchanging information on the use of the Internet for terrorist purposes and to identify possible strategies to combat this threat, while ensuring respect for relevant international human rights obligations and standards (MC.DEC/3/04). They further decided, *inter alia*, to intensify their action by enhancing international co-operation on countering the use of the Internet for terrorist purposes […] and to explore the possibility of more active engagement of civil society institutions and the private sector in preventing and countering the use of the Internet for terrorist purposes (MC.DEC/7/06).

Most recently participating States adopted Permanent Council Decision No. 1063 on an OSCE Consolidated Framework for the Fight Against Terrorism (December 2012). The Consolidated Framework lists, *inter alia*, countering the use of the Internet for terrorist purposes as strategic focus area for OSCE counter-terrorism activities in line with relevant OSCE counter-terrorism commitments and existing mandates. In addition, it underscores as a comparative advantage in the field of anti-terrorism the OSCE's comprehensive approach to security as well as its framework for multi-stakeholder dialogue, awareness-raising, exchange of expertise, good practice and lessons learned.

The TNTD/ATU has assisted OSCE participating States with their commitments in the field of combating terrorist use of the Internet by organizing and facilitating four OSCE wide events as well as three national workshops since 2005. The comparative advantage of OSCE efforts related to terrorist use of the Internet is that they are embedded within the organization's broader efforts to promote a comprehensive approach to cyber/ICT security. It allows looking at a specific perpetrator group in a cross-dimensional and integrated way that recognizes the interlinkages of cyber threats and perpetrators, and stresses the need for human rights compliant responses. In practice, this flexibility allows the TNTD/ATU to think outside the box, to make use of in-house expertise and to offer a "rounded" platform to share information on this topic, offering host countries an opportunity to take stock of overall national cyber/ICT security efforts and identify potential gaps.

2012 Online Forums

The 2012 online expert forum discussions were designed to reinvigorate and stimulate information exchange on the latest trends and debates related to terrorist use of the Internet, and to shed light on online activities by terrorists and their motives. The online forums focused on four topics: 1. The Internet used as tactical facilitator by terrorists (21-25 May 2012); 2. Terrorist abuse of social networking tools (2-6 July 2012); 3. Right wing extremist/terrorist use of the Internet (17-21 September 2012); and 4. Effective public private partnerships to counter terrorist use of the Internet (8-12 October 2012).

Discussions for each forum were based on discussion papers prepared by the TNTD/ATU and circulated to participating States prior to the forums. In this report they were used as introductions to the summary of the various discussions streams of the forums. The discussion papers were elaborated in close co-ordination with other relevant OSCE executive structures such as the Office for Democratic Institutions and Human Rights (ODIHR) and the Representative on the Freedom of the Media (RFoM). In addition, a group of internationally renowned experts and close contributors to OSCE activities in this field volunteered to review discussion papers as well as contribute significantly to the forums' discussions including by acting as "Introducers" or "Discussants". The online forums were conceptualized and moderated by the TNTD/ATU Action Officer for issues related to Countering the Use of the Internet for Terrorist Purposes (Ben.Hiller@osce.org).

IV. Cross Cutting Issues: Human Rights

A guiding principle during discussions was that any debate about addressing and finding answers related to the challenges emanating from terrorist use of the Internet needs to be anchored in the OSCE participating States' commitments to uphold human rights, in particular the right to privacy (including data protection), freedom of religion and belief, and freedom of expression enshrined in various OSCE consensus documents[2], including politically binding commitments.

OSCE participating States have repeatedly acknowledged the crucial link between effective counter-terrorism strategies and the respect for human rights, and that counter-terrorism measures which do not protect human rights are counter-productive. They have committed to prevent and combat terrorism in full compliance with international human rights standards.

Part and parcel of such an approach is that radicalization and extremism should not be targeted by law enforcement counter-terrorism measures, if they are not associated with violence or other unlawful acts, as legally defined in compliance with international human rights law (for instance, when groups considered to be radical or extremist do not resort to, incite or condone criminal activity and/or violence). Holding views or beliefs that are considered radical or extreme, as well as their peaceful expression, should not be considered crimes per se.

The forums reiterated that on the Internet a fine balance has to be struck between security and fundamental freedoms, whereby security measures need to be temporary in nature, always be decided by independent courts of law, narrowly defined to only meet a clearly set out purpose, prescribed by law and should not restrict legitimate speech or be used for imposing a monitoring obligation.

[2] For an overview of pertinent commitments please consult p. 7 of http://www.osce.org/fom/80723

Forum I: The Internet Used as Tactical Facilitator by Terrorists

Mobile devices, location based services, electronic financial transactions and social networking platforms can provide near universal situational awareness. The Mumbai terrorist attacks in 2008 have shown how terrorists take advantage of the consumerization of Information Technology (IT) in the preparation phase and execution of attacks. While the Internet has had tremendous positive effects on the world's population, tech-savvy terrorists found ways to use vastly enhanced commercial technology to provide them with affordable versions of the command, control, communications, computing and intelligence systems previously only available to nation states. The forum looked at how terrorists can use the Internet in the planning and execution of attacks, and focused on pertinent solutions. Forum discussion focused on four key themes: 1.) Balancing law enforcement needs and fundamental freedoms; 2.) Uncluttering intelligence information and human resources needs to collect actionable data, 3.) Effectively enlisting support from Internet users ; and 4.) how will the Internet shape future terrorist activities. [3]

Background

The terrorist attacks in Mumbai in 2008 which left 164 people dead demonstrated how the Internet was vital both in the planning stages as well as during the execution of the attacks. During the planning phase, the terrorists conducted virtual reconnaissance of their targets using online map services, enabling them to plot their mission with great precision, including determining entrances and exits to be used at the primary target locations and finding out geographic coordinates for their targets, which were programmed into GPS devices.[4]

Once the attack was underway, the terrorists used their Blackberry phones to provide status updates to their handlers as well as to receive instructions and updates from them such as on the location of hostages, the international reaction to the attacks, as well as on the police response[5]. The handlers themselves used VoIP channels to mask their physical locations. The level of tactical detail that transpired from social media services such as Twitter or Flickr from the public provided additional instantaneous situational awareness for the attackers, and concerned by the possibility that such activities aided the terrorists, the Indian authorities even posted a tweet themselves asking for live Twitter updates from Mumbai to cease immediately.[6]

On the other hand, the web proved to be a vital source of information, especially for the victims hiding in the hotels. Real life information on the attacks communicated through social media services provided a picture of what was going on and became one of the few sources of information for the hostages on the steps of the terrorists.[7] As such the siege

[3] The discussants of this forum were:

[4] http://apdforum.com/en_GB/article/rmiap/articles/print/features/2011/04/01/feature-01

[5] ibid

[6] http://news.bbc.co.uk/2/hi/south_asia/7752003.stm

[7] http://www.ngonlinenews.com/news/mumbai-attacks-and-social-media/

became a social media experiment as both terrorists and victims as well as the general public in India and beyond used the Internet and mobile devices to gather as much information as possible. It showed that everyday technology can be fundamental to carrying out terrorist attacks, but also proved that access to the Internet is crucial for gathering and exchanging of information, for enabling communication amongst citizens and in times of crisis can even be life saving.[8] However, the Mumbai attacks and the use of the Internet as a tactical facilitator for terrorists also threw up serious questions for law enforcement services on how to deal with this new component of terrorist attacks.

Challenges

<u>Intelligence Gathering</u>

Terrorists like the Mumbai attackers can analyse data from different sources and are able to summarize it into useful tactical information. Such information can derive from open source material such as location map services or tourist websites, but also from password protected social networking sites. The key for terrorists is to fuse seemingly non-harmful information from multiple sources to a complete picture that provides tactical situational awareness. Recognizing how apparently trivial personal information can be abused, the US army recently warned service personnel about the dangers of "geo-tagging". Specifically, the army leadership pointed out that smartphones had built-in GPS and that photographs were automatically embedded with the latitude and longitude of where the photograph was taken – information that could be advantageous to terrorists who are in command of the right software.[9] Likewise, social media platforms now allow users to tag locations with posts. Combined with updates on an individual's daily activities, and an oftentimes lax policy of many social networkers when it comes to accepting friend requests or when disclosing their own private data, social media platforms potentially allows terrorists to exploit Internet users to their advantage. This open source reconnaissance creates challenges for law enforcement authorities since such types of terrorist activities are unlikely to be flagged. As such relevant proactive, effective, and human rights compliant counter measures will likely have to involve the co-operation of the public as has been recognized in many countries as well as private online services providers.[10]

<u>Strategic/Tactical Communication</u>

New technologies and communication forms on the Internet and ways of accessing it, including Voice over Internet Protocol (VoIP), social networking fora, virtual worlds and micro-blogging translate into enormous amounts of communication data, and potentially allow terrorists to mask and hide tactical communication behind the "noise".[11] For instance, conventional tracing techniques to track a call from a land line or a mobile phone to a VoIP subscriber only allows law enforcement to get as far as the switching station that converts

[8] Ibid

[9] http://www.army.mil/article/75165/Geotagging_poses_security_risks/

[10] For instance the UK has established an Internet Referral Unit following up on complaints by the public on suspected terrorist online activities

[11] http://www.un.org/es/terrorism/ctitf/pdfs/ctitf_interagency_wg_compendium_legal_technical_aspects_web.pdf

the voice call into Internet data.[12] Moreover, while in many countries ISPs are required to retain Internet data for a certain period of time, the same rules do not often apply to VoIP records. In addition, terrorists can also make use of data encryption, multiple encryptions and steganography either commercially available or designed by terrorists for terrorists.[13] There is also evidence that terrorists are increasingly using the Bluetooth personal area network system to broadcast on a localised pocket-to-pocket basis - communication that is "below the radar" of law enforcement and intelligence agencies.[14] The multitude of communication channels, encrypted or not, can test law enforcement capabilities considerably faced with finite resources. While authorities are capable of collecting vast amounts of data, intercepting and decoding terrorist communication data in a human rights compliant manner requires considerable technical expertise, and a large pool of trained personnel to obtain actionable intelligence.

Diversification of Internet Access and Data Storage

Smartphones and the availability of non-registered SIM cards in many countries allow terrorists to use the Internet without any form of identification required.[15] In addition, due to their size, smartphones can be easily pick-pocketed and disposed of after fulfilling their purpose, adding to the already existing challenges of law enforcement to trace online activities to a particular individual. Moreover, cloud computing enables terrorists to host digital content in jurisdictions with little international co-operation history and consequently with little fear of identification.[16] As such cloud computing represents an additional grey area in terms of international law-enforcement co-operation and jurisdictional responsibilities. Experts have also pointed to another technique, among others, namely fast flux hosting – a technique which continuously moves the location of a website, email or domain name system server from computer to computer and could potentially further assist terrorists.[17] On the response side the diversification of mobile devices and storage capacities complicates law enforcement investigations and forensics considerably. Not only are mobile device forensics applications and toolkits relatively new, developers also have difficulties in keeping up with the emerging technological advances.[18] In more general terms, the pace of developments is also directly related to the training needs of law enforcement, politicians, and the judiciary.

Attribution, Anonymity and the Need for Trustworthy Forms of Identity

The extensive use of the Internet by the Mumbai terrorists to plan and carry out the attacks completely undetected underlined, yet again, one of the biggest obstacles in the fight against cyber misuse – anonymity, and consequently the challenging task for authorities to attribute with absolute certainty cyber activities to a specific perpetrator. A recent compendium by the UN Counter Terrorism Implementation Task Force (CTITF) Working

[12] http://www.nytimes.com/2008/12/09/world/asia/09mumbai.html
[13] http://www.reuters.com/article/2008/01/18/us-internet-islamists-software-idUSL1885793320080118
[14] http://eandt.theiet.org/magazine/2011/07/terrorisms-invisible-propaganda.cfm
[15] http://www.un.org/es/terrorism/ctitf/pdfs/ctitf_interagency_wg_compendium_legal_technical_aspects_web.pdf
[16] ibid
[17] http://www.icann.org/en/news/announcements/announcement-26jan09-en.htm
[18] http://articles.forensicfocus.com/2011/08/22/the-challenges-facing-computer-forensics-investigators-in-obtaining-information-from-mobile-devices-for-use-in-criminal-investigations/

Group on *The Use of the Internet for Terrorist Purposes – Legal and Technical Aspects* noted that more trustworthy forms of identity in cyberspace would be required in order to have any deterrent effect on terrorist use of the Internet.[19] This note is of particular importance since the Internet can also empower citizens and can potentially accelerate democratisation processes and allow citizens to access political, cultural and social information.[20] The ethical questions associated with online anonymity and the likely time it will take to come up with pertinent technical solutions, may underscore the need for certain rules of behaviour in cyberspace complemented by Confidence Building Measures (CBMs). [21]

Discussion Summary

Stream 1: Balancing Law Enforcement Needs and Fundamental Freedoms

The vast amount of communication data indicates that law enforcement responses to countering terrorists using the Internet as a tactical facilitator needs to be proactive rather than reactive. This must not be at the expense of human rights and fundamental freedoms.

- Experts stressed that the prevention of terrorists using the Internet as tactical facilitator goes parallel with significant challenges for law enforcement and anti-terrorism agencies. Offenders can use anonymous communication technology or public Internet access points (like Internet cafes) to hide their identity. In addition, they can use encryption technology to hinder access to the content of communication as well as stored data. This anonymity led some countries to introduce intensive investigation instruments e.g. Section 49 of the United Kingdom's Regulation of Investigatory Powers Act 2000 (RIPA) orders a suspect to disclose passwords to encrypted material. Different jurisdictions came to different conclusions how this affected fundamental human rights, especially the ban on self-incrimination. In addition, laws that require suspects to surrender keys to encrypted material often fail to take into account new technologies such as "Truecrypt" that allow hiding content even if passwords are surrendered.

- While controlling all terrorist/criminal online content is unrealistic and experts stressed that it is better to maintain an open Internet and to collect evidence to prosecute rather than shutting down websites, at times invasive measures are indispensable, especially if activities cross certain red lines e.g. inciting violence or imminent danger. However, such measures including blocking websites or taking down material - often viewed as controversial by the public - need to go in parallel with clear cut national laws and policies that respect fundamental rights and clearly lay down what threats justify what measures. In addition, it is important to establish an effective system for oversight that provides the opportunity for the affected party to complain if wrongfully targeted. Policies related to invasive measures need to involve and solicit the contributions by the public and civil society. This is important

[19] http://www.un.org/es/terrorism/ctitf/pdfs/ctitf_interagency_wg_compendium_legal_technical_aspects_web.pdf

[20] http://www.fco.gov.uk/en/news/latest-news/?view=Speech&id=685672482

[21] See e.g. pertinent work by the OSCE and PC.DEC No.1038 on the Development of Confidence-building Measures to reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies

in order to demystify what authorities are seeking to achieve and avoid risking a public relations backlash which in turn creates opportunities for terrorists. Likewise authorities need to be mindful how such efforts impact on international co-operation.

- While experts generally agreed with the importance of invasive measures to tackle terrorist online activities especially if it threatens national security, taking pertinent action internationally proves more difficult, or potentially makes matters worse in the absence of a harmonized international legal framework. For instance, a country's law enforcement response to a websites hosted in a third country might not only be perceived as an attack on national infrastructure, it could also interfere with an on-going police investigation. In addition, what one country considers being an acceptable emergency response opens the doors to a wide range of responses from other countries that have may have different yet valid concerns about other types of content.

- Experts underscored the importance of harmonizing the international legal framework to afford effective cross-border co-operation. However, this would only be a first step. The speed and transnational nature of the Internet constantly pushes traditional international co-operation to its limits. For instance, an expert quoted the company PayPal stressing that only in the rarest of cases "data has been returned to the requesting law enforcement agency in under three months. Six months is more common (…) and cases where data has been returned more than two years after it was originally requested. Given the speed at which cyber-attacks move, this effectively hobbles the investigating law enforcement agency and frequently cripples investigations."[22] Experts therefore called for more direct communication lines between law enforcement agencies as well as indirect co-operation through diplomatic missions to ensure timely responses and to ensure an adequate response to terrorists using the Internet as tactical facilitator.

- Experts stressed that international organizations might be an ideal place to evaluate potential invasive measures not only in terms of their compatibility with fundamental freedoms but also with regard to evaluating the costs and benefits of such measures.

Stream 2: Uncluttering Intelligence Information

In times of budgetary constraints, trained human resources capable of analysing an ever growing amount of communication data need to be as effective as possible.

- Experts pointed out that intelligence gathering as part of countering cyber threats needs to take into account the human factor. While authorities are technically capable of collecting vast amounts of data, there are inherent problems with large quantities of data in that the technical capacity to sift through that data in a

[22] https://www.paypal-media.com/assets/pdf/fact_sheet/PayPal_CombatingCybercrime_WP_0411_v4.pdf

meaningful way has not been developed in the same pace. Especially in emergency situations trained staff is therefore key since 1.) it takes a lot of maturity, technical know-how and analytical skills to deal with ad hoc cyber-intelligence; and 2.) once intelligence is understood, there is a need to act on it including in co-operation with partner authorities and countries. Hence training and capacity building of intelligence staff in the above areas is key. In addition, experts should be trained of how to make best use of Open Source Intelligence including as a means to triangulate and falsify "bad" information.

- Experts also pointed out that not enough use is being made of the advantages of public-private partnerships (PPPs) related to intelligence gathering and intelligence sharing. To make better use of the wealth of knowledge the private sector possesses, authorities need to establish clear-cut co-operation policies, laws, mechanisms and procedures. Likewise it is important for both sides to establish focal points as single points of contacts as part of ensuring timely co-operation.

- Experts reiterated that there already are international networks that allow for the sharing of intelligence and information related to cybercrimes and terrorist use of the Internet. Yet some experts felt that while such mechanisms are a sound co-operation platform, their effectiveness is at times limited due to their affiliation to certain international legal instruments which not all participating States are party to. Moreover, the very nature of intelligence and associated safeguards does at times hinder sharing it internationally.

Stream 3: The Role of the Internet User

It is often the individual Internet user who is the weakest link in terms of combating terrorist using the Internet as tactical facilitator, for instance by being careless about personal information. It is also the individual Internet user who is key in the prevention of online terrorist activities that could lead to potential attacks.

- Experts stressed that before looking at the user as key contributor to preventing terrorist using the Internet as tactical facilitator, it is necessary to clarify the current role and status of users and their degree of empowerment. For instance, one could argue that it is unreasonable to expect ordinary Internet users to expertly manipulate, manage or make informed choices about the complex array of technological tools and software solutions available today. In fact most users rely on the knowledge, skills, professionalism, legal and regulatory structures, technological know-how and engineering prowess of a wide range of intermediaries to deliver clear unambiguous policies, trusted hardware and software solutions based on democratic principles which provide reliable, trustworthy and respected products for use of ordinary users. In contrast one could argue that it is the user who expertly manipulates the technological spoils of the Internet age in devious ways e.g. to plan and carry out terrorist attacks. These reflect the behaviour of users and not the technology itself. Users therefore may have a responsibility to learn more about the tools they own, to understand what is possible and to take reasonable steps to protect their systems from attack and to prevent their hijack for use in an attack against others. Arguably users need to understand the acceptable use of this technology in everyday society and need to realise that illegal behaviour has consequences.

- A key question that was discussed was user liability. In this regard a key debate focused on the feasibility of a) developing some sort of online "driving licence" and b) whether this could practically be done. Experts stressed that while users do not know how their car works, they still possess a driving licence gained through achieving a certified proven understanding of the rules of the road and the capabilities of a motor vehicle, understanding that it needs regular maintenance, knowing how to achieve repairs for road-worthiness and accept their responsibility to put fuel into the car, change tire-types based on the seasons and to report when the vehicle has been in an accident or stolen. While experts stressed that something similar might be desirable for using the Internet and protecting computers, they also pointed to the considerable challenges this would entail such as who would be responsible for certifying online behaviour, how to enforce such a system nationally and internationally both technically and administratively, and how to reprimand misbehaviour. In addition, questions were raised whether it was actually desirable for authorities to prevent individuals from using the Internet, and what impact this could have on the freedom of expression and other fundamental rights.

- Experts agreed that cyber education was vital. Raising awareness and educating the individual Internet user on how to stay safe online throughout people's lives is essential and can turn internet users into the strongest link in terms of cyber security. Such initiatives should start at the beginning of a child's educational career including e.g. by passing an exam on cyber security, and continue throughout working life and retirement age. Experts suggested for the OSCE to play a key role in encouraging States to implement such educational programs and to offer capacity building assistance in this regard. Some experts even suggested for the OSCE to assess and rank the quality of national cyber education to create incentives for countries with lower rankings to invest more. As a first step the OSCE could consider facilitating the sharing of national school curricula on cyber education.

- Experts stressed that the private sector could also do more to encourage responsible online behaviour by Internet users. For instance, many online forums have already developed methods of supporting and encouraging good behaviour and discouraging bad behaviour. This is often done through a sort of merit/badge reward system or providing users with a number of 'ranks' or 'stars' which publicly acknowledge their contributions and good forum behaviour. Such mechanisms could be extended.

- Experts also discussed the potential role of users to detect terrorists and terrorist activity online. In this respect they discussed the added value of crowdsourcing[23]

[23] Crowdsourcing is a process that involves outsourcing tasks to a distributed group of people. This process can occur both online and offline. [1] Crowdsourcing is different from an ordinary outsourcing since it is a task or problem that is outsourced to an undefined public rather than a specific body http://en.wikipedia.org/wiki/Crowdsourcing#cite_note-howedefinition-3

especially in emergency situations. For instance a future area to look into is how crowdsourcing is used for identifying terrorist suspects in the immediate aftermath or preceding an imminent attack to help law enforcement agencies to identify suspects or to prevent an attack from happening. However, some doubts were voiced how effective users are in detecting and reporting terrorist online activities. For instance, citizens may not always the best judge of what is terrorist activity as opposed to e.g. extreme views. Hence if such help is enlisted such complaints should probably not go directly to police but to some sort of "middle person/entity" with the necessary expertise and experience to triage and prioritize the reports received.

Stream 4: Impact of the Internet on Future Terrorism

The Internet and an ever growing number of access tools have given terrorists a potential tactical advantage that has never been seen before the existence of the Internet. The question is how technological advances will impact on future terrorism.

- Experts agreed that new developments related to the Internet have the potential to further complicate the already highly complex landscape for intelligence, law enforcement, and policymakers tracking terrorist operations in cyberspace. Key concerns focused on what impact the sharp increase in the use of brand name commercial social networking services such as YouTube, Twitter, and Facebook by terrorist organizations and their supporters could have; how the continued exploits of hacktivists such as Anonymous and LulzSec could influence and motivate terrorists; what impact new technologies such as darknet or P2P filesharing could have on terrorist operations; how counter measures by governments and cyber vigilantes on terrorist websites impact their technological evolution.

- Experts also discussed how the spread of social networking technology can be leveraged in support of counter radicalization to more effectively stem the tide of terrorist recruitment online in the future. Talking about counter measures in more general terms, experts also pointed to the adaptability and willingness of cyber evildoers to learn. An enhanced skillset in turn impacts on the already finite resources of law enforcement agencies. In this respect experts also pointed out that terrorist already looked to other cybercriminals to increase their skills – a trend likely to continue in the future. For instance in June 2011, Al-Qaida's As-Sahab Media Foundation released a video titled "Thou Are Held Responsible Only for Yourself". In the video, As-Sahab dedicated a lengthy segment to the field of "electronic jihad" highlighting that those possessing hacking skills should use them. Similarly, FBI Director Robert Mueller said that terrorists had shown a clear interest in pursuing hacking skills and that they would either train their own recruits or hire outsiders, with an eye towards coupling physical attacks with cyber-attacks.[24] In this regard the black market is likely to play an increasingly important role for terrorists. For

[24] http://www.fbi.gov/news/testimony/fbi-budget-for-fiscal-year-2012

instance a recent Forbes article showed that 0-day exploits are already being traded for as little as $5,000 and up to $250,000.[25]

- Experts pointed out that the absence of a harmonized legal framework is likely to amplify existing challenges related to international co-operation; so too will differential interpretations on where to draw the line related to imposing restrictions that are justified, proportionate, based on the rule of law and necessary in a democratic society. In this respect one expert stressed that even if there were adequate laws, the nature of the Internet is such that it would lead to a never-ending “cat and mouse” game to track down such content. Having said that the expert also stressed that an obvious red line should be incitement to violence, or content that grossly contrasts with the universal value of human dignity. In the long term a more effective strategy to tackle incitement to terrorism might be to make more "positive" use of the Internet by matching hatred in equal quantity and quality with counter-narratives. In this regard authorities have an important role to play, but perhaps more as an engine, encouraging civil society to join the “frontline”. The breadth and the credibility that is required for effective messaging are such that public-private partnerships are indispensable.

[25] http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/

Forum II: Terrorist Use of Social Networking Tools

A recent report highlighted that 90% of terrorist activity on the Internet takes place using social networking tools.[26] That terrorists are using the Internet is not new; that nearly their entire activity takes place in the relative openness of social networking is a relatively new finding. Terrorists appear to transform low cost and easily accessible social media into a strategic facilitator to communicate, network, incite, glorify and plan. As such, social media can potentially act as a force-multiplier enhancing the organizing capabilities of a terrorist group, its ability to shape the public narrative as well as attract the attention of potential new recruits.[27] The forum sought to solicit answers on potential response by law enforcement; the role of the Internet user in responding to this threat and the role of the private sector.

Background

Uses of Social Networking Tools

Traditionally terrorist online content was one-directional and text based, either in the form of websites or text and messages posted on forums. In comparison, social networking tools and platforms including chatrooms, social networking sites, blogs, video-sharing sites, allow terrorists to assume a more proactive role.[28] Social networking tools could be used by terrorists for:

- **Recruitment/Incitement**: Instead of waiting for potential recruits to come across websites hosting terrorist propaganda based on hear-say, terrorists can now directly contact potential recruits or lure individuals to their sites via social networking platforms. As such these platforms offer terrorists an added security layer and an opportunity to "vet" potential recruits. Likewise, social networking tools can be used by "interested" individuals to disguise identities e.g. by posing as someone else when contacting terrorists. Once an emotional, psychological or intellectual bond has been established between terrorist and potential terrorist the path to more hidden online content and communications can be cleared.[29]

- **Planning/Strategic Communication:** Terrorists can analyse data from different sources and are able to fuse it into useful tactical information to plan potential attacks, or for use during an active terrorist campaign. For instance, they can potentially take advantage of careless personal data disclosures of Internet users on social networking sites including updates on an individual's daily activities, geo-tagged posts and pictures while exploiting an oftentimes lax policy of social networkers when it comes to accepting friend requests. Moreover, as the Mumbai

[26] Weimann, Gabriel, 2011, *Al Qaeda Has Sent You A Friend Request: Terrorists Using Online Social Networking*
[27] http://soufangroup.com/news/details/?Article_Id=272
[28] Weimann, Gabriel, 2011, Al Qaeda Has Sent You A Friend Request: Terrorists Using Online Social Networking
[29] ibid

terrorist attacks from 2008 showed, the level of tactical detail that transpired from social media services such as Twitter or Flickr from the public demonstrated that blogging services can provide instantaneous situational awareness for the attackers, circumventing traditional law enforcement counter measures such as blocking mobile phone networks.

- **Public Outreach/Glorification:** Terrorists have learnt to use social networking platforms to propagate their cause and to shape the public narrative before or shortly after attacks. Terrorist organizations such as al Qaeda have designated media offices and attacks are frequently filmed and uploaded only moments after they occur.[30] They offer their version of reality, often glorifying violence and perceived successes. In turn, such activities both potentially fuel societal fear as well as are likely to impress likeminded individuals - often resulting in both tactical and strategic gains to the terrorist operation and the overall terrorist cause.

Social Networking Tools

Networking tools that can be abused by terrorists include:

- **Chat Rooms:** Chat rooms enable "netizens", NGOs, civil society groups, but also terrorist groups to communicate with like-minded people and supporters all over the world, to recruit new followers and to share information at little risk of identification by authorities. For instance, free chat room service PalTalk, which includes voice and video capabilities, has become particularly popular with terrorists.[31] In addition to being used to generate support, chatrooms are used to share tactical information with "experts" directly answering questions on issues such as how to build a bomb or how to hack into computer systems.

- **Blogs:** A report by the U.S. Army's 304th Military Intelligence Battalion stressed that blogging services such as Twitter can represent an effective co-ordination tool for terrorists trying to co-ordinate attacks – as was witnessed during the 2008 Mumbai attacks. The report further highlights further possible scenarios of terrorist usage of this online format including receiving near real-time updates on the location of potential targets or e.g. hacking into an account of a soldier communicating with other soldiers under a stolen identity.[32]

- **Social Networking Sites**: Virtual communities are growing increasingly popular, especially among younger demographics. Social networking websites allow terrorists to reach an impressionable age bracket that might empathize with their cause. In addition, many social network users are careless when accepting friend requests which could allow terrorists to access personal information. There are also various terrorist groups that have open pages on social networking sites and anyone

[30] See e.g. http://www.npr.org/templates/story/story.php?storyId=5548044
[31] Weimann, Gabriel, 2011, *Al Qaeda Has Sent You A Friend Request: Terrorists Using Online Social Networking*
[32] http://afp.google.com/article/ALeqM5jGd91R-NdcJLa8N6OBU76hbrVFyg

interested can read the information, look at the discussion boards, link to propaganda videos and join the group.[33]

- **Video Sharing:** Terrorists make use of video hosting/sharing online platforms[34] and convicted terrorists have openly praised its usefulness for attracting funding, inciting to violence, and propagating activities.[35] In addition, a study on posts and comments related to online videos concluded that online videos reached global audiences, particularly younger viewers and as such terrorist content was spreading far beyond what might be conceived as its core support base.[36]

Discussion Summary

Stream 1: Enhancing Law Enforcement Responses

Given the budgetary constraints, trained human resources capable of analysing and responding to terrorist use of social networking tools need to be as effective as possible.

- Experts stressed that communication forums and social networks increasingly appear to be both advantageous and disadvantageous: While terrorists realised their potential to use them for communication, networking, incitement, glorification and operational planning, law enforcement can leverage these tools as well to gain greater insight into terrorist activities while also being able to collect evidence for prosecuting perpetrators of criminal activities. Experts underscored that most fundamentally, responses must take into account due legal process, data protection, discrimination, privacy and profiling concerns and at the same time guarantee the freedom of opinion and expression and the right to free assembly.

- Given the value of information posted on a social networking site, law enforcement analysts throughout the world are already tracking Twitter and Facebook posts to collect intelligence as part of countering terrorists abusing social networking sites - a very labour intensive activity. Given the large volume of data, some law enforcement agencies are investing in the development of digital tools that can scan the entire spectrum of social media enabling them to acquire more data. Experts stressed that such technology was vital considering the ratio of law enforcement officers to cyber evildoers including terrorists.

- However, questions were raised how useful such tools are: Many experts said the major hurdle is in teaching computers how to read. For instance, how can software distinguish between valuable information and subtleties in meaning as opposed to a

[33] Weimann, Gabriel, 2011, *Al Qaeda Has Sent You A Friend Request: Terrorists Using Online Social Networking*

[34] E.g. http://news.sky.com/home/uk-news/article/15210314

[35] http://www.telegraph.co.uk/news/worldnews/northamerica/usa/3547072/JihadistforumJihadist--calls-for-YouTube-Invasion.html

[36] Conway, Maura, and Lisa McInerney, 2008. "Jihadi Video & Auto-Radicalisation: Evidence from an Exploratory YouTube Study". In *Proceedings of the 1st European Conference on intelligence and Security informatics*, Esbjerg, Denmark, 3-5 December 2008.

"joke". Moreover, authenticity is also a problem when it comes to computer programs known as spam bots which already plague services such as Twitter with junk posts similar to email spam. Many experts feel that the ability to create spam bots will only improve over time potentially fooling analysts and their software into thinking they're witnessing a genuine activity when it's entirely artificial and meant to mislead. In addition, tracking technology without defining a narrow and targeted law enforcement purpose is also questionable from a human rights and fundamental freedoms perspective; even if information is publically available and no specific groups or person are targeted. Experts also underscored that at the end of the day it will still require trained officers to sift through the data generated by technology or outside sources and to take action.

- Experts debated whether it is more effective for law enforcement to employ proactive measures or preventive/reactive measures when countering terrorist use of social networking tools – often referred to as the shutdown vs. exploit question. For instance one experts pointed to a recent study by Cambridge University which concluded that strategic campaigns targeting criminal networks might actually be a more cost efficient way to strengthen cyber security. In contrast other experts pointed to the international "legal minefield" that not only made such responses difficult but in addition such intrusive measures could also impact negatively on future international co-operation. As such some experts felt it is more important to look into harmonizing the international legal framework first, and stick primarily to preventive working level measures including joint law enforcement investigation agreements e.g. in the framework of organizations such as the CSTO.

- Experts also suggested that law enforcement should rely more or consider closer ties with the private sector and pertinent efforts to combat malicious activities. For instance one expert pointed to Microsoft's Digital Crimes Unit. The Unit currently focuses on disrupting some of the most difficult cybercrime threats – including technology-facilitated child sexual exploitation and malicious software crimes, particularly botnet-driven Internet attacks. It does so in close co-operation with industry, law enforcement, academia, governments, and NGOs worldwide. [37]

Stream 2: Empowering Internet Users and Civil Society

Social networkers are key in terms of preventing and addressing terrorist use of social networking tools.

- Experts highlighted that the concepts of "last line of defence" and "first responders" offer good starting points to envisage the role and empowerment of end-users in addressing terrorist use of social networking tools. End-users arguably have a key interest in a safe and secure social media. As first responders, users should be able to recognize instances of terrorist abuse of social networks, and feel encouraged to report such instances to social media operators, competent state authorities and/or

[37] http://www.microsoft.com/government/ww/safety-defense/initiatives/pages/digital-crimes-unit.aspx

civil society organizations. As the “last line of defence”, individual users should be educated about responsible online behaviour, privacy issues and the risks associated with the disclosure of personal data and other potentially sensitive information through social media. Individual users should also be resilient to messages and content disseminated through social media which are violent or which are potential precursors to violent attitudes.

- Experts highlighted the special role of civil society organizations (CSOs). CSOs have a crucial role to play in strengthening end-user resilience to violent content, and in efforts to win “hearts and minds”. Importantly, CSOs can often build on legitimacy, credibility and latitude that state authorities may perhaps not have, especially in tackling non-violent extremism. They should be encouraged to leverage social media to drive the formulation and dissemination of positive messages and counter-narratives that challenge terrorist propaganda and hate speech.

- Social media offers unique advocacy tools for CSOs in terms of empowering counter-voices, innovative packaging and targeted outreach to appeal to specific audiences. For instance social networking tools can be used to bring together end-users and other stakeholders, e.g. former violent extremists and victims, as part of building participatory communities around positive values. Similarly, CSOs could be involved in monitoring and referral mechanisms to identify and address suspicious contents/activities, including the delivery of ‘online preventive interventions’ to engage with at-risk end-users.

- Experts pointed out that several social networking operators offered mechanisms that could be utilized by users to flag content that violates the community guidelines or terms of service. However, it is unclear how often such features are actually used and how much staff is devoted to screen such content. It is also unclear to what degree companies actually raise users’ awareness of these features and encourage them to make use of them. In fact encouraging the use of such mechanisms may be counter-productive and costly for operators and a reputational risk. As such future debates needed to focus on the one side how to encourage users to make use of such options and secondly what incentives could be created for operators to actively promote such systems.

- Experts pointed out that a particular challenge in educating Internet users in the secure use of social networking tools is the dynamic environment of the Internet itself. For instance, Facebook did not exist a decade ago, and Twitter is barely five years old. Another challenge is to encourage users to actually make use of their cyber security knowledge. Hence cyber education needs to focus both on practical measures but also behavioural change i.e. to encourage users to behave in secure way over a long period of time. In that regard incentives are crucial to reinforce good behaviours from time to time.

Stream 3: The Role of the Private Sector

Since most social networking tools are owned by private companies, transparent, institutionalised and mutually beneficial public-private partnerships are essential for preventing terrorist abuse of social networking tools and in the interest of social networking providers.

- Experts pointed out that the responsibility for preventing and countering terrorist use of social networking tools lies primarily with national authorities. Hence potential obligations imposed on social networking operators to monitor social networks or enhanced liability of the private sector to prohibit, take down or notify authorities are not appropriate. However, experts also highlighted that the private sector does have a business interest to contribute and find mutually agreeable co-operation solutions.

- In order to get broad scale buy in from the private sector it was suggested to appeal to social networking operators' corporate social responsibility and their interest to protect their image/reputation. However, when looking into reputational issues authorities should be sensitive to the fact that social network owners/operators may be wary of appearing in the eye of users/clients as agents or proxies for governments.

- It was pointed out that many providers have already introduced various initiatives to keep their networks clean from terrorist material e.g. by taking down terrorist propaganda videos. However, such responses were sketchy and different guidelines were applied by different owners. One idea in this respect was to develop voluntary guidelines that could be applied across the board and offer a certain degree of sustainability. In this respect it is important to think about incentives to encourage long term compliance (i.e. positive reinforcement) including potential (business) benefits e.g. reputational gains, reduced administrative costs, or privileged access to extra resources/support.

- Experts pointed out that a lot of private companies already engaged in efforts to formulate effective PPPs. However, it always tended to be the same private companies willing to contribute to such processes. Hence experts wondered whether there is not only a need to look into enhanced public private partnerships but also enhanced private-private partnerships. Specifically, from a public sector point of view it would probably help if there would be some form of umbrella organization/spokesperson endorsed by the majority of private companies. Another idea was for the private sector to have rotating intermediaries as contact points for the public sector as well as international organizations looking into facilitating better co-operation. These way most private operators could be involved and the costs could potentially be shared among the private sector.

Forum III: Right Wing Violent Extremism/Terrorist Use of the Internet: Emerging Patterns and Differences

Investigations including in connection with recent high profile incidents in the U.S. and in Europe related to right-wing violent extremism/terrorism unearthed a diverse picture of the threat level stemming from such groups/individuals, their organizational make-up as well as their coherence. For instance, according to EUROPOL, extreme right-wing terrorism remains less significant than other forms of terrorist activity.[38] In contrast, the UK Parliament Home Affairs Committee concluded that there is compelling evidence about the potential threat from extreme far-right terrorism.[39] Part of the difficulty to establish the extent of the threat could be different ways of recording such crimes and conflicting concepts related to right wing violence.

Regardless of this, experts agree that the cost of right-wing violent extremism on the Internet should be of concern to all.[40] For instance, EUROPOL argued that the Internet and in particular, online social media and the development of online pan- European networks - both of which proved important in cases such as Anders Breivik- are "adding a new dimension to the threat right-wing extremism may present in the future."[41] Taking into account such factors as a worsening economic situation, an enhanced connectivity and cohesion could accelerate a radicalization process that could lead to violence. Addressing the underlying causes for radicalization and responding to right wing violent extremist/terrorist use of the Internet therefore appears to be vital, regardless of differing estimates on the threat level stemming from right wing violent extremists/terrorists.

Questions the forum sought to address included how right wing violent extremists/terrorists use the Internet, how does it differ from other terrorist use of the Internet, and what are potentially effective responses to this threat including taking into account good practices in countering other forms of violent extremism online.

Challenges

Right Wing Violent Extremism vs. Terrorism vs. Hate Crimes?

When reviewing expertise on right-wing terrorism and/or violent extremism (including use of the Internet) the dividing lines between concepts can at times appear blurred. Violent extremism, hate crimes, and terrorism are often used as synonyms to describe the use of violence by several actors within the right wing ideology.[42] For instance, the Institute for Strategic Dialogue concluded in a recent conference paper that "right wing violence is defined in different ways across Europe and security agencies record acts of violence in

[38] https://www.europol.europa.eu/sites/default/files/publications/te-sat2011.pdf

[39] http://www.publications.parliament.uk/pa/cm201012/cmselect/cmhaff/1446/144610.htm

[40] http://www.iiuedu.eu/press/journals/sds/SDS_2011/DET_Article2.pdf

[41] https://www.europol.europa.eu/sites/default/files/publications/te-sat2011.pdf

[42] http://www.transnationalterrorism.eu/tekst/publications/Rightwing%20terrorism.pdf

different ways,"[43] which makes it difficult to assess the real threat and to compare trends. Moreover, the report stressed there is little clarity at what point groups or individuals may move from sporadic acts of right wing extremist violence to planning terrorist activities[44], and arguably what role the Internet plays in this regard. It appears that right-wing violence emanating from some forms of terrorism, violent extremism and hate crimes can all be motivated by biases and prejudices held by actors within the right wing ideology. Yet differences can/do exist in terms of the intensity of violence, the goals, the intended targets as well as pertinent responses. Arguably in terms of responses they may depend on how national authorities categorise any given right-wing violent crime.

Interplay between Different Forms of Violent Extremism and Prevention Efforts

Right wing violent extremism has predominantly been addressed through the prism of hate crimes, while al Qaeda type violent extremism and radicalization has been viewed through terrorism lenses. The question is in how far prevention efforts related to preventing right wing violent extremism and al Qaeda inspired violent extremism do/can/should overlap. For instance, the UK Parliament Home Affairs Committee recommended that when responding to right wing violent extremism/terrorism the potential interplay between different forms of violent extremism should be acknowledged, and the potential for measures directed at violent far-right extremism to have a consequential effect on other forms of violent extremism and vice versa.[45] Hence, it appears that at times different brands of violent extremism are in a symbiotic, mutually reinforcing relationship. The spread of violent extreme right ideas, and the resulting discrimination, could actually be a factor conducive to al Qaeda inspired radicalization, and vice versa. OSCE participating States too have recognized "the role hate crimes, discrimination and intolerance can play in fuelling violent extremism and radicalization that lead to terrorism"[46]. However, the cross-fertilisation of prevention efforts, including on the Internet, targeted at the ideological underpinnings of terrorism or right wing violent extremist ideas have been limited so far.

Confusing Picture on the Cohesion and Co-ordination of Right Wing Violent Extremists/Terrorists

A third challenge, which is to some degree connected to the above two, is the uncertainty about how well connected and co-ordinated right wing violent extremists/terrorists are, both nationally and internationally, and what role the Internet plays in this regard. For instance the EUROPOL TE-SAT 2011 report highlighted a lack of unity and a lower degree of overall co-ordination of right-wing terrorists and/or violent extremists compared to other terrorist groups.[47] Yet a recent report by anti-racism-group Hope Not Hate identified a contrasting picture with regard to online activities. The report found that so called "counter jihad groups" that inspired Anders Behring Breivik were growing in reach and influence on the Internet. Importantly, far-right organisations were becoming more cohesive as they forged alliances throughout Europe and the U.S., with 190 groups now identified as

[43] http://www.strategicdialogue.org/RadicalRight_Conference.pdf
[44] ibid
[45] http://www.publications.parliament.uk/pa/cm201012/cmselect/cmhaff/1446/144610.htm
[46] http://www.osce.org/cio/40695
[47] https://www.europol.europa.eu/sites/default/files/publications/te-sat2011.pdf

promoting an Islamophobic agenda.[48] Taking into account a potential interplay between various forms of violent extremism, the current economic situation and the precedent Breivik could have set for such groups, it would not be too far-fetched to expect further cohesion and momentum which could lead to violent extremist acts or attempts to coerce third parties into responding or amending policy.

Discussion Summary

Stream 1: How do right-wing violent extremists/terrorists use the Internet and what trends can be noted?

While organizations such as EUROPOL note that the Internet adds a new dimension to the threat emanating from right wing violent extremism/terrorism, currently there is insufficient understanding of how exactly this is manifested.

- Experts pointed out that right wing violent extremist online activity is increasing. For instance one expert stressed that in his country a tendency could be observed that right wing groups were increasingly politicizing their perceived grievances targeting authorities rather than hate crime specific targets i.e. foreigners – a tendency that was also fuelled by radical political groups. However, responding to such online propaganda and activities is as difficult as any other form of violent extremism or xenophobia, not least because content often originates from other countries. The continuous absence of a harmonized international legal framework continues to hinder effective international co-operation.

- Experts stressed the use of the Internet by right wing extremists did not differ all too much from other extremist groups. Currently three levels of online activities could be observed: Level one involves the use of social media outlets such as Twitter, Facebook or YouTube to post propaganda videos and publications; Level two is semi-public, consisting of dedicated websites for the dissemination of propaganda and some web forums with both public and private sections; and level three is often referred to as the ‘deep’ or ‘dark’ web and consists of password-protected forums which are often hidden using file repositories and storage sites.

- Experts pointed out that recent years have seen far right use of the first level expand, with an abundance of social media methods employed by the extreme right. An example is the ‘Immortal’ group in Germany, which organises exclusively through Twitter and other social media outlets to stage unregistered rallies, and uses YouTube to disseminate footage of the gatherings. Semi-public forums such as ‘Stormfront’, founded by a former Ku Klux Klan leader in the 1990s, make up the second level. The third level is made up of password-protected forums such as Legion88.

- Experts identified al Qaeda inspired terrorists primarily use the Internet as follows:

[48] http://www.guardian.co.uk/world/2012/apr/14/breivik-trial-norway-mass-murderer

  - Virtual media organisations have been major sources of dissemination of al Qaeda type publications and audio-visual materials.
  - These websites have sought to narrow the credibility gap between established news media and themselves by mirroring mainstream and established media sites.
  - The use of new social media by extremists and terrorist networks is becoming more common and significant to these groups. There is some evidence to show that al Qaeda type violent extremists are employing social media as part of a formal strategy.
  - Online activities need to be understood in conjunction with offline events. Though the internet is a key component of the radicalisation process, it is a weak tool for actual recruitment of terrorists into an organisation and for training. This nearly always takes place offline and face to face.
  - The Internet has allowed the proliferation of instruction manuals, detailing everything from how to build an IEDs to how to produce poison gas.
  - There are cases known where terrorists have engaged in online credit card fraud, identity theft and other illegal activities to fund their operations.
  - The Internet offers greater opportunities for women to become active within such circles than simply offline engagement.

- Experts identified that right-wing extremist use of the Internet exhibits several similarities to that of al Qaeda type extremists:

  - Extreme right wing websites are sophisticated, and are often hosted outside their target jurisdictions to avoid legal sanctions.
  - The online proliferation of instruction manuals has also been used by the far right.
  - There are reasons to believe that women are more likely to engage with right-wing extremist sites and become active within far right circles than they might in the offline space, though there is less data to evidence this.

- Experts also identified some distinct characteristics of far right use of the Internet:

  - Rather than mirroring established media news outlets to gain credibility, extreme right websites heavily target youth, reflecting a young lifestyle and employing recognisable styles, slogans, and symbols.
  - The extreme right capitalises on relationship-building mechanisms online, and the emergence of new social media and other such tools has become far more important than static websites. Building a sense of comradeship or family is key.
  - The far right radicalisation process online is focused largely on promoting racial narcissism, building indifference towards potential victims, and fostering a sense of credibility and power among fringe groups.
  - The online space is a major source of funding for right-wing movements. Many websites merchandise white power and Nazi paraphernalia, and right-wing Internet shops are on the rise.

Stream 2: What can be learnt from combating al Qaeda inspired terrorism online in responding to right wing violent extremism/terrorism on the Internet?

While it is important to recognize and deal with hate crimes and other forms of extreme right wing violence as separate, distinct issues, especially in terms of education, awareness raising, law enforcement and justice agency response, the question of possible overlap between preventing such expressions of violence and preventing terrorism nevertheless arises.

- Some experts pointed out that the concept of "lone wolf" terrorism appeared to apply particularly to right wing violent extremists/terrorists as could be recently observed in Norway, which made responses more difficult. Responses were also made more difficult by the fact that right wing extremists tended to be less overtly violent in their expressions. For instance, while al Qaeda inspired forums often clearly incite violence and as a result can be taken down, right wing forums flourish, since views expressed in them may be objectionable but are often not illegal, even if they potentially fuel violent notions.

- Experts pointed out that it might be useful to focus on extremism without affiliating the concept necessarily to an ideological/religious motivation/cause. This could prevent authorities to overtly focus on one group or another as was the case in recent years with some forms of violent extremisms being neglected or less researched.

- Experts suggested for the OSCE to help to identify and enhance data sharing on potential tipping points when extremist views turn violent. The idea being that some baseline knowledge is available that can be used to counter different forms of extremism from turning violent irrespective of the motivations behind holding extreme views. In this regard it is also important to intensify efforts to compare methods and identify commonalities between different forms of counter measures to tackle different forms of extremism e.g. counter narratives vs. countering xenophobic statements and why they are effective or not. This would allow future efforts to start from a solid foundation whatever the political/ideological direction of potential new violent extremist groups.

Forum IV: Institutionalising Public-Private Partnerships (PPPs) to Combat Terrorist Use of the Internet: Getting the Balance between Public and Private Contributions Right!

Effective PPPs are considered a necessity both by the public and private sector to combat terrorist use of the Internet. Most of the Internet infrastructure including communication systems and platforms are privately owned, yet it is largely in the hands of state authorities to act upon its misuse.

In reality, however, the relationship is often unequal, on an ad hoc basis, and rarely formalised. There are a number of challenges associated with such co-operation, including the borderless character of the Internet; different national laws related to terrorist use of the Internet; limited knowledge of each other's expertise, and many more.

In the middle is the individual Internet user – both in his/her role as "first responder" by detecting terrorist use of the Internet e.g. on social networking in the first place, and reporting it, as well as in his/her role as "last line of defence" through responsible and privacy conscious use of the Internet thereby preventing possible abuse. As such effective PPPs to combat terrorist use of the Internet are three-way relationships between authorities, Internet companies as well as Internet users and by extension civil society organizations.

The forum looked at how balanced public-private partnerships look like, and what pertinent preconditions are; and the role of Internet users as well as civil society.

Challenges

Clear Cut Policies and Legislation

Countering terrorist use of the Internet can be challenging from a legal perspective.[49] The very nature of the Internet makes cross-border co-operation necessary both between authorities and between law enforcement of one country and a private company in another. This can at times lead to competing national laws, arguably all of which are applicable in cyberspace.[50] In terms of potential terrorist crimes on the Internet and associated content it is often difficult to determine what is "illegal". The illegality of content might differ between countries in turn limiting the effectiveness of cross-border co-operation e.g. between law enforcement and Internet related companies. In addition, labelling content might be too short-sighted in some instances. For instance, whereas content that is deemed "illegal" might not actually fuel terrorism, content that can be considered "legal" may potentially be

[49] See e.g. http://www.un.org/en/terrorism/ctitf/pdfs/ctitf_interagency_wg_compendium_legal_technical_aspects_web.pdf

[50] See e.g. http://95.211.138.23/documents/

harmful e.g. the spread of non-violent extremist views[51]. Apart from the legal issues, government policies related to combating terrorist use of the Internet do also differ in extent, comprehensiveness, and applicability, and how well they are communicated to the private sector on a national but also international basis,[52] making it potentially difficult for Internet related companies to evaluate co-operation requests. Finally, while there may well be several effective co-operation mechanisms between law enforcement and the private sector on a national basis, they may differ in detail from each other, which makes synergies on an international level difficult.

Clear Cut Roles and Responsibilities

In the simplest of terms co-operation between the public and private sector is indispensable not least due to the very distinct roles each sector fulfils. The primary focus of national authorities is on legal issues - be it to criminalize terrorist use of the Internet or to prosecute criminal activities, in line with human rights and fundamental freedoms. In contrast, Internet related companies are providing a service, often focusing on technical issues. While most companies are willing to assist in preventing and combating terrorist use of the Internet,[53] it may not necessarily be their task to determine what is and what is not legitimate use of their services e.g. in terms of online content or act as a judge when it comes to privacy concerns, nor may they have the capabilities and resources to do so. Nevertheless keeping the Internet safe from terrorist use is in the interest of both sectors - and both sectors need to pull their weight in a mutually beneficial way. For instance, Internet related companies can be and are proactive in terms of making clear to its users that terrorist use of the Internet will not be tolerated, and encourage reports on misuse which in turn are forwarded to law enforcement agencies. In turn, authorities should clearly spell out expectations to the private sector keeping in mind each other's roles and responsibilities. One very visible option reflecting co-operation without meddling with areas of responsibilities is to enhance the visibility of law enforcement e.g. on social media platforms in form of virtual police controls to remind users that criminal use of the Internet is not acceptable.[54] Likewise, appointing points of contacts for terrorist use of the Internet within authorities and the private sector can enhance continuous information exchange.

Engaging with the Internet Users

The Internet is simply too large to leave it to law enforcement and Internet related companies to effectively respond and prevent terrorist use of the Internet. It requires the active involvement of Internet users and civil society. As such effective public-private partnerships need to consider how to most effectively engage with Internet users and civil society to strengthen their roles as "first responders" and "last line of defence". As the last line of defence, individual users should be educated about responsible online behaviour, privacy issues and the risks associated with the disclosure of personal data and other

[51] Holding views or beliefs that are considered radical or extreme, as well as their peaceful expression, should not be an object for law enforcement counter-terrorism measures as long as they are not associated with violence or another unlawful act, as legally defined in compliance with international human rights law

[52] See e.g. Council of Europe Country Reports on combating Terrorist Use of the Internet: http://www.coe.int/t/dlapil/codexter/cyberterrorism_db.asp

[53] See e.g. http://www.un.org/apps/news/story.asp?NewsID=33874&Cr=terror&Cr1=?ref=enews250210

[54] Similar e.g. to http://www.dailymail.co.uk/news/article-1360908/Virtual-police-patrol-Facebook-hunt-cyber-bullies.html

potentially sensitive information. As first responders, individual users should be able to recognize when they are confronted with instances of terrorist use of the Internet and feel encouraged to refer suspicious activity and content to the responsible authorities and/or Internet service, while being resilient to terrorist content in the first place. It is especially the latter where civil society organizations play a crucial role. Both authorities and Internet related companies individually or jointly have created a number of mechanisms and tools to solicit the support from Internet user to e.g. report or flag misuse ranging from Internet Referral Units,[55] to flagging options on social media platforms or website.[56] Their effectiveness, however, is not always clear. Internet users are often not used to report what they believe to be terrorist use of the Internet.[57] Moreover, by installing flagging options it is often up to Internet related companies to determine the legality of reported terrorist activities e.g. on their platforms and what content to refer to law enforcement agencies even though they may lack specialist knowledge.[58] Effective PPPs therefore need not only consider how to share the responsibility to engage with the public most effectively and strategically, but also to consider how to most effectively engage with Internet users to respond to terrorist use of the Internet, including in co-operation with civil society organizations.

Discussion Summary

Stream 1: Mutual Beneficial Public-Private Partnerships

How do balanced public-private partnerships look like, and what are pertinent preconditions? How can such co-operation be institutionalised e.g. through general co-operation principles, including on the international level?

- Experts pointed out that public-private partnerships are not the "silver bullet" to end terrorist use of the Internet but represent a widely shared recognition that the public and the private sector must work together to achieve certain goals including counter-terrorism efforts not least because current regulatory approaches are often insufficient. Such collaborative governance structures can be set up at the local, national, or international/multinational level focusing on different extremist groups and regions. Key to such efforts was to recognise each other's roles and responsibilities and that co-operation is mutually beneficial.

- It was highlighted that project focused public private collaborations tend to be more successful. They usually have a clear deadline creating a sense of urgency among the participating actors and therefore channelling their activities in a common direction. This also makes it easier to raise the resources required to achieve the goal and to secure senior leadership support. Deadlines make it easier to avoid potential difficult legal questions by including sunset clauses and temporary provisions. And successful

[55] See e.g. http://www.reuters.com/article/2010/10/04/us-security-internet-factbox-idUSTRE6932AY20101004
[56] See e.g. http://www.facebook.com/help/search/?q=report+links
[57] See e.g. http://95.211.138.23/documents/
[58] ibid

projects are “easier to sell” to superiors in both the private and the public sector contributing to an individual’s personal professional and career advancement goals and therefore also ensuring greater buy-in.

- Process focused public private partnerships on the other hand are a greater challenge and require institutionalizing collaborative governance structures. The challenge here is to create a common perception of the problem that leads to a shared interest. Senior leadership support is key in this regard to lay the foundation as well as to reinvigorate the partnership during times of weak leadership. Triggering moments offer opportunities to initiate and institutionalize such partnerships. It is important that value is created for both sides so that participants see a return of investment on their time and resources.

- A key element of a successful collaboration is trust between private and public sector officials. This requires openness among participants to work together as a precondition in order to overcome initial mistrust. And there are clear limits to effective trust-building within a social group: The larger a group’s membership, the harder it will be to establish and maintain trust over time. A successful institutionalization of a partnership therefore requires an investment over time by a group of people to regularly interact and work together and importantly trust each other.

- It was pointed out that non-legislative ´frameworks´ such as the Clean IT Project could facilitate sustainable and effective co-operation. In essence, the Internet industry, NGOs, law enforcement and governmental organizations agree on key principles and best practices related to countering terrorist use of the Internet serving as guidelines for future efforts thereby filling the gap between (national) regulation and private initiatives / best practices. Key to elaborating such principles and guidelines is to include the public in consultations and to afford as transparent of a process as possible until all parties can agree on a set of principles and implement them. Experts did stress that at times and in some situations more formal agreements were needed.

Stream 2: Role of the Internet User/Civil Society

How can Internet users and civil society be involved most effectively? What are current good practices and how can existing tools and mechanisms to enlist individual Internet users be enhanced?

- Apart from potential contributions in the previous fora, experts reiterated the potential value of Internet users and civil society to tackle online extremisms. A good example is the Against Violent Extremism network. It is itself the offspring of a larger public-private effort represented by Google Ideas, a think/do tank set up by Google with a public service mission. Specifically it is a global network of former violent extremists, survivors, activists, policy makers and business people united by a common mission: to counter violent extremism. The business model is to focus on a particular topic each year, convene a major expert-level summit, and to then channel the energy into an institutionalized organizational off-spring that will continue to focus on the topic down the road. Hence it starts with a project-focused approach which then transitions into a process-oriented collaboration. It also combines the insights from sociology and trust among small groups with a network structured approach to achieve a high level of scope at the same time.

- It was highlighted that another way users could contribute to countering terrorist use of the Internet was a form of volunteering or doing community service as part of crowdsourcing efforts. This could include actively encouraging others to report malicious activities.

- Experts stressed that one key obstacle reporting terrorist use of the Internet was that reporting mechanisms are mostly confined to national boundaries. Experts suggested for international organizations such as the OSCE to look into ways how reporting mechanisms could internationalised or centralised so that reported content is automatically referred to the responsible national authorities. In addition it is important to standardise and simplify reporting mechanisms so that users actually make use of it.