Responding to Terrorist Use of the Internet and Cyberspace

Camino KAVANAGH,[a1] Madeline CARR, [b] Francesca BOSCO[c] and Adam HADLEY[d]
[a]*King's College London/ ICT4Peace*
[b]*Cardiff University*
[c]*UNICRI,* [d]*ICT4Peace*

Abstract. The authors of this paper consider recent developments involving terrorist use of the internet and cyberspace for a range of purposes, as well as renewed concerns relating to potential terrorist attacks against critical infrastructure and their control systems. Following from an overview of recent trends, they discuss public and private efforts to respond to existing and emerging threats. The authors anchor these within the context of current efforts to manage a range of interrelated cyber security challenges, focusing predominantly on the international and regional response, as well as efforts by industry actors to deal with terrorist use of their products and services.

Keywords. Terrorism,[2] counter-terrorism, internet, ICT, cyberspace, Islamic State, al Qaeda, law enforcement, United Nations, private sector, norms, practices.

1. Introduction

As far back as 1990, experts at a United Nations (UN) conference on the implications of technology for international security in Sendai, Japan, forecast some of the difficulties UN member states would confront in efforts to manage the diffusion of political, scientific and technological power enabled by the information technology revolution. The report emerging from the conference stressed that the international community was not well positioned to deal constructively with some of the disruptive side-effects stemming from the diffusion of science and technology throughout the world, noting that the very distribution of technologies that we encourage may also give strength to certain forces which we wish to suppress - notably terrorism, sub-national violence, ethnic and religious intolerance [2].

---

[1] Corresponding author. Department of War Studies, 6th Floor, King's College London, Strand, London, WC2R 2LS, UK. Email: camino.kavanagh@kcl.ac.uk.

[2] Since there is no universal agreement on a definition of terrorism, the authors have chosen to lean on the EU Council Common Position 2001/931/CFSP and the Council Framework Decision 2002/475/JHA which defines 'terrorist offences' as acts committed with the aim of 'seriously intimidating a population', 'unduly compelling a government or international organization to perform or abstain from performing any act', or 'seriously destabilizing or destroying the fundamental political, constitutional, economic or social structures of a country or an international organization'. For a broader discussion of the definitions issue, see the document published by the European Parliament in November 2015 [1].

Fast-forward some two decades. The worldwide population is approximately 7.5 billion and growing. The societal dependency on information technology identified at the end of the Cold War has significantly increased. The internet – commercialized in the mid-1990s – has some 3.56 billion users [3]. Some 2.3 million Google searches are conducted per minute and 6,000 tweets are sent every second.[3] As of January 2016, Google has reportedly indexed some 17 trillion web pages. Today there are 2.3 billion social media users. The past year alone has seen a rise of 200 million users, 1.5 billion alone on Facebook. Internet users maintain an average of six social media accounts. And there are 1.65 billion active mobile social accounts globally.

This level of connectivity brings important advantages:

- It connects people across borders (physical, linguistic, economic, etc.);
- It allows much greater access to information and enables the transfer of knowledge in various forms (text, graphics, video, audio, etc.);
- It enables a rapid flow of information for business, education and so forth at unprecedented speed;
- It constitutes an environment where information can be passed anonymously through the use of certain tools and techniques; and,
- It gives users access to a global audience at a relatively low cost.

Yet, this level of connectivity has also represented a drop in the institutional scale required to both challenge the state and do real harm. Any number of actors – either state or non-state, powerful or weak – can exploit the largely decentralized and open nature of the internet, the low-cost means of communication, as well as freedom of expression and access to information that it allows.

Beyond the internet, dependency on ICT for the functionality of critical infrastructure (CI) systems has also increased. Indeed, over the course of the past quarter century, two developments have resulted in many countries relying heavily on cyberspace for the operation and delivery of heavily interconnected and interdependent infrastructure systems. The first development was, of course, the rapid evolution of networking technology that facilitated the connection of these large systems. A second development was the trend in many jurisdictions to privatise management of critical infrastructure, which introduced a more explicit profit motive into their operation [5]. Today, a number of sectors such as transport, banking, communications, health, food and water and their underlying infrastructure are highly enmeshed with the different technologies that constitute cyberspace [6].

A combination of considerations around managing expense and expectations of consistent delivery has meant that many of the systems put in place in this context are not as robust as they could have been. Taking critical infrastructure systems offline to upgrade them, even briefly, can be very costly and disruptive. In addition, the interconnected and interdependent nature of the systems complicates efforts to protect one single critical infrastructure, as does the fact that there is no agreement between and within states on which infrastructure is actually 'critical'. Critical infrastructure and its dependence on cyberspace has thus been regarded as a key asset as well as a major vulnerability by policy makers for some time, with concerns relating to potential

[3] For instance, according to a *New York Times* article, when Egypt closed down the internet on 27 January 2011, traffic fell to under ten percent of its normal rate within a few hours [4].

terrorist attacks against critical infrastructures and their control systems ebbing and flowing in tempo with the marked increase in global terrorist activity.

2. Terrorism and the Internet

Given the manner with which non-state groups have harnessed information technology in the past for malicious purposes, it is perhaps not surprising that we have seen growth in the use of the internet for terrorist purposes in parallel with the growing pervasiveness of the internet and ICT in general, and the number of terrorism-related deaths (figure 1 below). What has been largely unexpected, however, is the enthusiasm with which these groups have embraced these tools. Many of the terrorist groups that have emerged in recent times have become adept users of the internet - particularly social media platforms – to meet their aims. For the sake of clarity, the authors have clustered these uses under two umbrellas – propaganda-related content and communications and operations-related content.

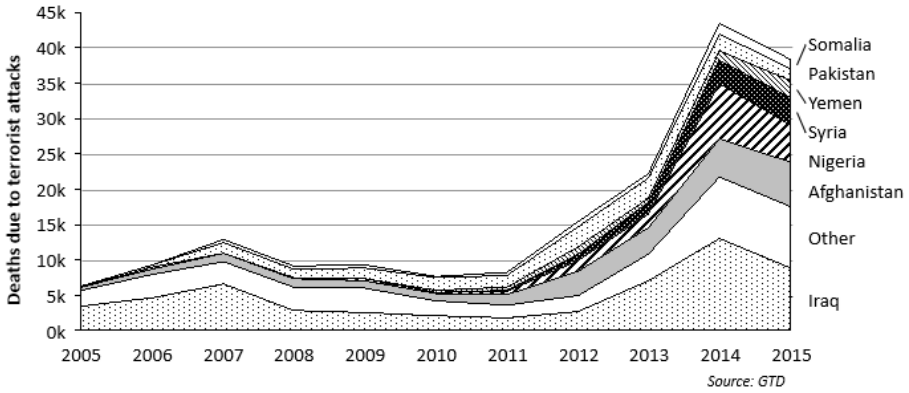

Figure 1. Number of terrorism-related deaths

2.1 Propaganda Related Content and Communications

Using different forms of information technology to communicate, develop and distribute terrorist-related content or to plan, fund and execute operations is not a new phenomenon. Like organised crime, modern-day terrorist groups have been quick to adapt to technological innovations. Today, groups such as the so-called Islamic State (IS) have taken full advantage of the decentralised nature of the internet and the core principles of openness and freedom of expression underpinning it. They use it for strategic communications and propaganda, including for promoting extremist causes and for providing a seemingly infinite source of content that can be picked up by the mainstream media. They also use it to harass and intimidate, incite violence and spread fear among the global public.

IS's glossy online magazine *Dabiq,* styled along the lines of *Time Magazine,* is evidence of the nature of the content produced by these groups. Another recent example is *Kybernetiq*, a German language publication produced by IS, which teaches

information security and operational security to IS militants, or the recently-launched *al-Fatihin* (meaning 'Conquerors' in Arabic) publication launched on 20 June 2016 with the tagline: 'The newspaper for Malay-speaking migrants in the Islamic State'. The *al-Fatihin* articles provide updates from battle theatres of Iraq and Syria, targeting potential recruits in the Malay-speaking nations of Southeast Asia.[4]

Similar online activity has been, and continues to be, employed by other internationally-recognized terrorist organizations, such as al-Qaeda, however the level of sophistication and the full intensity with which IS carries out its online activities are unmatched. Al-Qaeda in the Arabian Peninsula's (AQIP) online publication, *Inspire,* for example, famously circulated bomb making instructions, which were claimed as a source of inspiration for the Boston Marathon bombers in 2013. Additionally, al-Qaeda and al-Shabab have notably used social media, particularly Twitter, as a tool for their recruitment strategies and general propaganda dissemination, using a number of languages as a means to attract a wider audience. Many other groups have, at a minimum, been able to develop an official website, communicate and spread information via forums, and produce low-quality media.

With the establishment and continuous development of its *Al Hayat Media* entity, IS has, nonetheless, ensured the production of better quality media publications and high definition videos. Openly accessible, *Al Hayat* also serves as a 'clearinghouse for jihadi primary source material, original analysis and translation' [7]. Beyond these self-styled 'jihadology' services [7], the group has also demonstrated a keen ability to utilize and develop specialized tools, such as the 'Dawn of Glad Tidings' app for a more effective dissemination of tweets, making the group stand out from among the others. Moreover, the graphic nature of the content posted by IS has become a target of interest for the media and the general public, via which the spread of publicity can lead to both an increase in recruitment and the spread of fear. Along similar lines, IS has used a hostage – British journalist John Cantlie – as a mouthpiece for the group on its 'Lend Me Your Ears' and 'Inside' series on YouTube, produced between 2014 and 2015. The use of a hostage to spread seemingly convincing propaganda, while painting a rosy picture of life inside the so-called Islamic State and criticizing the actions of legitimate governments, serves as a powerful tool for psychological manipulation and the spread of misinformation among the global public.

Sharing content online has also played against IS however. Azami notes how, for instance, its efforts in Afghanistan were thwarted following the release of a disturbing video in which ten blindfolded village elders were 'forced to sit on the ground on top of holes already filled with explosives' and blown up. The graphic video IS fighters posted spurred a concerted effort by the Taliban to drive IS out of Afghanistan, while also imbuing the Taliban with a sense of legitimacy and moderation vis-à-vis regional and international actors that it is capitalising on for purposes other than countering IS [8].

Nonetheless, beyond Afghanistan, there is an abundance of evidence demonstrating the group's adeptness at embracing the internet for propaganda purposes

[4] According to SOAS University of London, Malay in its various forms unites almost 200 million people into the fifth largest language community in the world (see: https://www.soas.ac.uk/sea/sealanguages/malay/).

at key moments, including in the immediate aftermath of terrorist attacks when the potential for further grooming, recruitment and radicalization is ripe.

2.2 Operations Related Content

From an operational perspective, IS and numerous other groups have become adept at using the internet to provide guidance and instruction, distributing to their followers and affiliates detailed information on which platforms to use to promote violence or transfer knowledge on the planning and execution of attacks, on the making of improvised explosive devices (IEDs) and other explosives, and on arms purchases and sales. Similarly, they use online platforms to raise or transfer funds and share information on which technologies to use to circumvent government monitoring and surveillance. And they continuously adapt their tactics and techniques to innovations in the world of technology, and to world events.

The latest spate of IS messages via Telegram, inciting potential lone wolves to conduct attacks against high level *kuffar* during the Rio Olympic Games, and how and where to buy arms to that end, are a case in point [9]. The earlier case involving US national Ali Shukri Amin provides insight into how IS supporters allegedly overcome challenges relating to fundraising and transfer of funds, using micro-messaging services to share suggestions on the most secure virtual currencies and fund raising platforms with those intent on 'commit[ing] jihad or travelling overseas' [10]. Mirroring the tactics of other IS members and supporters, the defendant allegedly created a blog on which he posted a number of 'highly-technical articles' targeting potential recruits and IS supporters, detailing the use of security measures in online communications to include use of anonymity software, tools and techniques [10].

Importantly, and as noted in the most recent 'Report of the UN Secretary-General on the threat posed by ISIL to international peace and security', neither the military nor the economic squeeze currently being effected against IS in the territories it controls, especially in Iraq and the Syrian Arab Republic, have been translated into a similar reduction of its active use of cyberspace and ICT [11]. If anything, its failing territorial strategy, coupled with the ongoing ideological conflict with al-Qaeda, appears to have driven an uptake in online activity.

Combined, these developments have sparked intense discussion and debate over how best to respond to terrorist use of the internet and cyberspace, particularly as terrorist activity continues to spread across the globe. Responding coherently to these developments and in a manner that balances existing tensions between national security prerogatives and hard-earned rights and democratic principles is no easy task.

2.3 Shaping a Response

Efforts to respond to terrorist use of the internet involve a number of cooperative, information exchange, and capacity building measures involving law enforcement agencies and diplomatic actors, as well as a range of policy, regulatory and technical actions directly or indirectly involving ICT industry actors.

Internet-specific actions include using big-data, and network, or real-time, social network analysis in support of traditional policing and surveillance. Some of these approaches bring with them a range of challenges (discussed in some detail below).

Other key actions include content-related regulatory measures (reflected in legislation, court orders or directives, or by-laws, some of which are often very vague). As will be discussed below, this increasingly involves using intermediaries to enforce regulations or compelling companies to block or filter specific content. Numerous states are also investing heavily in communications strategies aimed at countering the online narratives of terrorist groups and those intent on grooming, radicalizing or inciting violence.

2.3.1 Emerging Norms and Practices

At the national level, much of the ongoing strategic communications activity is centred on de-radicalisation and countering ideological messages. Many of these initiatives resonate with, or rather have their roots in, propaganda strategies developed during the Cold War. They are aimed at effecting behavioural and attitudinal change in certain communities and often lean heavily on civil society engagement as well as that of a range of private companies from different sectors. Initiatives such as COUNTER and PREVENT under the UK's Counter Terrorism Strategy (CONTEST), the US State Department's 'Think Again Turn Away' or the so-called 'Madison-Valley-Wood Project' campaign are just some examples of states' ambitions in this area but they encounter some significant challenges. Indeed, there are serious doubts about the capacity of governments (and others) to socially engineer their way around the ideological messages of terrorist groups, with many actions reported as further alienating targeted communities.

Issues related to the costs of these initiatives and their sustainability, including workforce and monitoring capacity abound. At the same time, engaging terrorist propaganda and allowing it to remain online can in some cases create hubs for terrorist content, which can be centrally monitored by law enforcement authorities, rather than having police constantly searching for new locations of extremist content following the shutdown of terrorist-related websites.

Other content-specific actions implemented by states include content filtering and, of course, surveillance (both covert and otherwise) and accessing user data held by companies.

At the international level, the G7 recently announced a range of actions in its 'Plan on Countering Terrorism and Violent Extremism' while a UN Security Council Presidential Statement ambitiously tasked the Counter Terrorism Committee with developing a proposal for a 'comprehensive international framework to counter the use of narratives by ISIL, al-Qaeda and other terrorist groups that encourage, motivate and recruit members to commit terrorist acts' [12]. The proposal is expected to include policy options for coordinating the implementation of the framework and mobilising resources around it.

A growing number of countries are using extra-legal restrictions such as requests to social media companies and other content hosts to monitor and take down content on their own initiative. To this end, government agencies use companies' terms of service (rather than, or in addition to, national legislation) to flag 'inappropriate' content as a means to prompt a given company to remove the flagged content or deactivate an account. As referenced in figure 2 below, these kinds of content removal requests have increased significantly in certain jurisdictions over time.

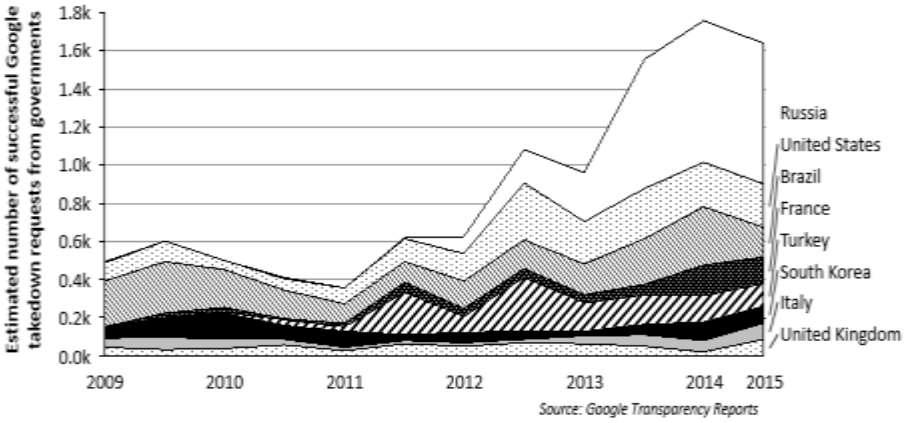

Figure 2. Content removal requests

Existing data points to important differences between government practices regarding content removal. Google transparency reports reveal that the number of requests by, for example, the Russian Federation have risen significantly since the middle of 2012. Indeed, as of 2015, its requests make up almost half of all government requests made to the company globally.[5]

In 2014, the European Commission established an Internet Forum aimed at working with private companies to respond to terrorist use of the internet. Within the framework of this initiative, it has supported the establishment of an Internet Referral unit (IRU) within EUROPOL. Modelled on the UK IRU, the EUROPOL unit is dedicated to reducing the level and impact of terrorist and violent extremist propaganda on the internet. Like the UK initiative, it is tasked with identifying and referring relevant online content to social media companies and internet service providers and supporting member states with operational and strategic analysis. Certain challenges relating to the *modus operandi* and the effectiveness of these initiatives have been raised, notably questions of transparency and oversight relating to the content being suggested for removal.

In 2015, and in response to the rising number of incidents relating to filtering, blocking and take-down of illegal content on the internet, the Council of Europe commissioned a comparative study on the topic across the organisation's 47 member states [13]. The report highlighted increasing and serious concerns about the absence of any legal basis to justify blocking content. The issue was developed further by the European Court of Human Rights judgment in the case of *Ahmet Yildirim v. Turkey* (no.3111/10), which held that that blocking access to an entire online platform was a violation of the right to freedom of expression. The Court also found that the legal framework in place in Turkey was inadequate and failed to provide sufficient safeguards against abuses [14]. In December 2015, a similar judgment dealing with a blocking order in Turkey of the popular video-sharing website YouTube found that the blocking of access to YouTube amounted to a violation of the right to receive and

[5] According to Google's transparency data, on average 60 percent of requests are partially or fully implemented by Google, although no distinction is made in the reports between partial and full compliance.

impart information under Article 10 of the European Convention of Human Rights (ECHR) [15].

2.3.2 The Role of Industry

Important debates have emerged over who holds ultimate responsibility for reporting and responding to terrorist online content. Engaging the private sector – ICT and ISP industry actors in particular - is evidently key to both national and international responses. Today, companies as diverse as Twitter, Facebook, Microsoft, VK, Weibo, WeChat, ASKFm, Instagram, What's App (and many, many more) are increasingly compelled to take action in response to how their products and services are used by terrorist groups or individuals inciting violence. Such action can include content removal via human or machine interaction (or a mix of both), engaging users to report or flag terrorist content, or working with governments or civil society to counter the narratives of terrorist actors. Although not specifically related to terrorist content, figure 3 below, which draws from transparency reports published by Facebook, Google and Twitter, demonstrates a marked increase in content removal requests over the past five years, generally conducted in response to the government requests or requests presented by individuals.[6]

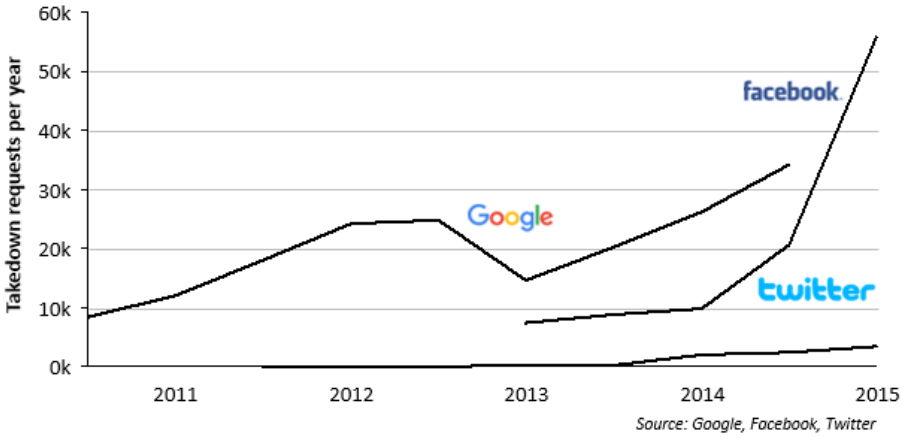

Figure 3. Takedown requests

In relation to terrorism-specific content removal requests and in the light of increasing pressure from governments (and often citizens), many companies have amended – or are in the process of amending – their terms of service to move beyond existing prohibitions of hate speech and advocacy of violence against others on their products and services to include the prohibition of terrorist content. This in itself is complicated since there is no universal definition of either terrorism or terrorist content. To overcome this barrier and for the purpose of its services, one major technology

[6] Google has published transparency data since at least 2011, with Facebook and Twitter following suit in 2013. Depending on the company, content removal requests can be broken down by nature of request and the originating country

company is studying whether to consider terrorist content to be 'any material posted by or in support of organisations included on the Consolidated United Nations Security Council Sanctions List and that depicts graphic violence, encourages violent action, endorses a terrorist organisation or its acts, or encourages people to join such groups'. Given the absence of common rules and standards, this approach might be the most viable at present. It will however need to bear in mind many of the existing challenges relating to listing, delisting and legal remedy, not least because it runs the risk of tempting certain governments to increase the number of persons, groups and entities they recommend for listing.[7]

Meanwhile, several companies have developed reporting tools allowing users (whether government, citizens or other groups) to alert them to terrorist content on their services. Of course, content can be taken down, but it can just as easily be re-posted elsewhere. In response to increasing pressure from governments, a number of companies are directly or indirectly (via third parties) using automation to scan, detect and remove terrorist content (notably images, audio and video) after it has been removed from one site. The objective in this instance is to avoid the game of 'whack-a-mole' that often occurs when content that is taken down soon reappears elsewhere, including on the sites of smaller companies that do not have the resources to monitor and remove content.

2.4 Contested Norms and Practices

It is too early to tell how effective any of these responses are. It is equally unclear how governments and/or companies intend measuring their impact or effectiveness, or how they will adapt to emerging challenges posed by existing and emerging technologies. It is, however, possible to identify where some of the challenges lie.

Just over a decade ago, UN member states had pledged to 'coordinate efforts at the international and regional level to counter terrorism in all its forms and manifestations on the Internet' [19]. However, as noted in a 2009 report of the UN Counter Terrorism Implementation Task Force (UNCTITF) Working Group, there is no single integrated approach to address the issue. The Council of Europe's Budapest Convention provides for law enforcement cooperation, but the instrument has only been ratified by some 49 states and lacks broader legitimacy, not least because its universality remains contested [20, 21].

In 2012, and in collaboration with the UNCTTF, the UN Office on Drugs and Crime (UNODC) launched a publication entitled *The Use of the Internet for Terrorist Purposes* - highlighting some of the core legislative and prosecutorial challenges states face in responding to terrorist use of the Internet. Intended as a resource for criminal justice practitioners and as a tool for capacity building, the report also stressed the need for to enhance cooperation between criminal justice systems and the private sector, as well as international cooperation, particularly increased cooperation between Governments 'in the investigation, detection, arrest, extradition and prosecution of those involved in terrorist acts. [22]. The UNODC study also highlighted the tensions

[7] Some of the challenges relating to the listing regime have been dealt with over the years, yet core challenges remain [16, 17]. For a more comprehensive review of UN targeted sanctions, see [18].

that were already emerging between policies focusing on security and those promoting openness and freedom.

Countering terrorist propaganda online continues to present a multitude of difficulties. The important disparities between different legal approaches to dealing with terrorist activity and content online persist. Many cases are prosecuted via *ad hoc* application of either existing cybercrime or counterterrorism legislation. The international cooperation required to investigate and prosecute such activity poses additional difficulties, as data is increasingly transferred and stored across borders with users, hardware and host provider located across different jurisdictions. This presents difficulties for detection, information sharing and other forms of law enforcement cooperation, as does the disparity of resources and expertise available to different national agencies. Furthermore, the principle of dual criminality also hinders effective countermeasures, as countries may not criminalize the same type of activity. Standards of proof, rules of evidence and sentencing also differ significantly across national boundaries. While the international frameworks currently being established to enhance cooperation on countering cybercrime may help overcome some of these challenges, their interpretation and application still varies widely from country to country [23].

A recurring question is whether it is more effective to suppress or engage terrorist use of the internet, especially propaganda activities. While the instinctive reaction of some government agencies is to shut down terrorist-related websites, such an approach is often counterproductive [24]. First, as highlighted above, suppression of terrorist-related propaganda is often a short-term solution that merely displaces content from one website to another, with a consequent waste of resources as analysts and investigators keep chasing a highly mobile target [25]. In addition, allowing extremist sites to remain online can provide law enforcement agencies with the capability to centrally monitor terrorist activity and prevent, or even disrupt, potential terrorist attacks by engaging in undercover sting operations.

Second, and as discussed further below, filtering and censorship sit uneasily with universal principles such as freedom of expression, and thus raise concerns from advocates of civil liberties and the public at large. Indeed, striking a balance between national security prerogatives and rights (particularly freedom of expression and opinion, privacy and the right to access information) is no easy task, even less so following the more recent increase in attacks.

Citizen concerns relating to the respect of core principles such as transparency and accountability abound, notably with regard to the surveillance and data collection practices of some states and the requests they make to companies relating to content removal, access to information and private accounts. In 2014 and in the light of some of these developments, the Council of Europe's Commissioner for Human Rights, Nils Muižnieks, released an 'Issue Paper' on 'The Rule of Law on the Internet and in the Wider Digital World' urging member states to:

> [e]nsure that any restrictions on access to Internet content affecting users under their jurisdiction are based on a strict and predictable legal framework regulating the scope of any such restrictions and affording the guarantee of judicial oversight to prevent possible abuses. In addition, domestic courts must examine whether any blocking measure is necessary, effective and proportionate, and in particular whether it is targeted enough so as to impact only on the specific content that requires blocking. Member states should not rely on or

> encourage private actors who control the Internet and the wider digital environment to carry out blocking outside a framework meeting the criteria described above [26].

The need for effective and more accountable public-private and multi-stakeholder engagement and concrete cooperation is widely recognized. Equally important is engaging civil society and academia in some of these public-private initiatives since their legitimacy generally derives from user values and interests. Failure to engage these groups can ultimately undermine the initiative, regardless of good intentions. For instance, on 31 May 2016, the European Commission and a number of technology and social media companies (including Facebook, Twitter, YouTube and Microsoft) announced the launch of a *Code of Conduct on Illegal Online Hate Speech*. Through the *Code of Conduct*, the companies involved have agreed to a number of commitments including:

- establishing clear and effective processes to review notifications regarding illegal hate speech so they can remove or disable access to such content in less than 24 hours;
- raising awareness with users about the types of content not permitted under their community guidelines;
- intensifying cooperation with other platforms and social media companies to enhance the sharing of practices; and,
- intensifying cooperation with EU member states and law enforcement agencies.

The process leading to the adoption of the *Code of Conduct* had initially involved a commitment to engage those key civil society actors with normative concerns relating to potential curbs on freedom of expression and opinion in shaping the *Code of Conduct* [27]. However, having been reportedly excluded from the final steps, a number of civil society organisations withdrew their support, claiming that it was 'established outside an accountable democratic framework, exploits unclear liability rules for companies […] and creates serious risks for freedom of expression as legal but controversial content may well be deleted as a result of this voluntary and unaccountable take down mechanism' [28]. It remains uncertain whether the initiative will survive.

Relatedly, important debate has emerged around the legitimacy of content removal efforts, even if geared toward undesirable terrorist content. As discussed, many government actions directly or indirectly involve the private sector, while a number of industry actors have taken it on themselves to determine what behaviour is permissible or not with regard to their products and services. The latter in turn poses important questions regarding oversight and participation in decision-making, both key principles of democratic governance. In response, since 2011, a growing number of companies are publishing regular transparency reports. One limitation of these reports, however, is that they are often published significantly after the fact (perhaps reflecting delays – legal or otherwise – encountered in implementing requests) and do not always provide much detail on the nature of the request or the content involved (often for legitimate security reasons). There is also a degree of ambiguity regarding the requests and the volume of content involved, since one single request can cover an unlimited number of articles, tweets, posts, or links. In addition, there is significant fragmentation of practice, with bigger companies better placed to respond to calls for greater transparency around their content removal practices. Initiatives such as the

Telecommunications Transparency Project and its *DIY Transparency Report* tool may help improve practice. The tool is specifically designed to help small and medium sized organizations produce holistic transparency reports and can certainly help explain to customers, citizens, and government agencies alike 'how an organization retains data, its policies for disclosing information to government agencies, and the regularity at which it does disclose information to such agencies' [29]. In short, clearer and more common standards, greater transparency and the continued sharing of good practices between both large and small companies, and continuous dialogue with the public could certainly help allay many existing concerns.

The recent report of the Special Rapporteur on Freedom of Expression on the role of the private sector in the digital age, released in May 2016, highlights the increasingly important role of the private sector, notably technology and social media companies, in the area of global governance. This greater role for commercial companies, the report argues, raises important questions – all of which remain unresolved – about applicable law and the scope of private authority and public regulation [30]. Such questions relate to the responsibilities of private actors and where these responsibilities should derive from (human rights law, terms of service, contractual arrangements or other), the parameters of relations between private actors and states, and the steps private actors should take when their actions risk interfering with core rights. They also relate to the role of governments and their growing reliance on private enterprise to achieve ends that are generally restricted by law.

In the light of some of these persistent challenges, in 2016 the UN Counter Terrorism Committee's Executive Directorate launched a project with the Geneva-based ICT4Peace Foundation to study these challenges in more detail. Its summary report from the first year of consultations with private sector actors, multi-stakeholder policy and normative initiatives such as that led by the Global Network Initiative [31], academia and civil society highlight the norms, standards and principles that companies (and governments) should bear in mind when managing terrorist-related content and activity online [32]. A second phase of the project which commenced in January 2017 will facilitate further dialogue between actors on these principles, collate emerging good practice (public and private) and make it available and accessible to a broader audience.

As for civil society organisations, their work on the applicability of universally accepted human rights online has made very important contributions to the debate on the need to protect rights while also ensuring public safety and national security. They too carry the responsibility of engaging a broader number of actors across the globe in their own work, for not all citizens, including victims of hate speech or terrorism, might agree with different groups' positions on content-related issues.

Finally, other not insignificant challenges relate to the growing reliance by governments on technology and technology-enabled solutions to resolve or manage highly complex issues such as radicalization and terrorism. Already in 2012 a UNCTITF Working Group Compendium highlighted a basic but fundamental fact:

> [t]echnology alone is no panacea for combating terrorism, including terrorist use of the Internet. Technical approaches should be enshrined in appropriate legal frameworks, which – in turn – should be part of a comprehensive public policy response that support and clarify the role of technology in combating and countering terrorist activity on the Internet [33].

Undoubtedly, the continued tendency toward technological solutionism tends to ignore the very structural issues that led to terrorist-related activity in the first place and relegates hard-earned principles such as participation, transparency and accountability in decision-making and national policy to a secondary role [34].

3. Beyond the Internet: The Threat of Terrorist Attacks Against Critical Infrastructure

The terrorist threat is no longer perceived to be just connected to terrorist activity on and through the internet. Just a few years ago, and counter to many who were predicting different forms of terrorist-enabled high-impact cyber attacks, experts across the globe remained sceptical as to the capacity and resources of terrorist groups to engage in such activity. Today however, a growing number of governments and cyber security experts have shifted tack, sharpening their tone in terms of the growing potential for non-state (and state) actors to engage in different modes of *intentional interference* [35]. The latter refers to acts of sabotage against either the critical IT/ICT infrastructure such as the global submarine fibre optic cable network or satellites, or cyber-enabled attacks against the industrial control systems (ICS), including SCADA (Supervisory Control and Data Acquisition) systems, of critical infrastructure [8] (communications, transport, nuclear, electrical power grids, dam facilities and other forms of energy supplies, manufacturing facilities and so forth).[9]

This concern stems from the growing realization that both state and non-state actors alike could use malicious IT tools and capabilities, directly or via proxies, to disrupt systems or to undercut traditional threat and warning indicators in order to create an effect; whether political, ideological, financial or other. While there remains a marked tendency to conflate IS's social media skills with the capacity and capabilities required to conduct a high-impact cyber-enabled attack against critical infrastructure, the demonstrated willingness of IS to commit violent acts both within and outside its area of military operations has convinced many experts that concerns are justified [37]. Just recently, a report on the work of the Global Initiative to Combat Nuclear Terrorism (GICNT) pin-pointed cyber terrorism (and groups such as IS) as a key threat, urging the GICNT to step up efforts in this area [36]. Meanwhile, a number of experts have highlighted the vulnerabilities of the global submarine fibre optic cable system to terrorist attack [38].

The UN General Assembly's Group of Governmental Experts (GGE) on developments in the field of information and telecommunications in the context of international security raised some of these concerns in its last report published in July 2015, noting specifically that:

> [t]he use of ICTs for terrorist purposes, beyond recruitment, financing, training and incitement, including for terrorist attacks against ICTs or ICT-dependent infrastructure, is

[8] Challenges abound around even defining critical infrastructure. In the US, CI is currently divided into 16 different sectors, many of which overlap.

[9] Today ICS products are mostly based on standard embedded systems platforms and they often use commercial off-the-shelf software. This results in the reduction of costs and improved ease of use while at the same time increasing the exposure to computer network-based attacks [36].

an increasing possibility, which if left unaddressed may threaten international peace and security [39].

For the European Union Agency for Network and Information Security (ENISA), reports of 'deliberate disruptions of critical automation systems' are evidence that attacks perpetrated through cyberspace can have a significant impact on CI infrastructures and services, with 'disastrous consequences for the EU Member States' governments and social wellbeing' [38]. Hence it has identified ensuring ICT robustness against cyber-attacks as a key challenge at national and pan-European level.

Although suspected of being sponsored by a state actor, attacks perpetrated against the control centre of the Prykarpattyaoblenergo power station in West Ukraine in December 2015 has since accelerated concerns relating to the potential of terrorist groups to commit similar acts.

3.1 Terrorism and Critical Infrastructure Protection - the Response

Responding to potential terrorist attacks against critical infrastructure is certainly no easy task. Moreover, the nature of many critical infrastructure sectors today – which are largely owned and operated by private concerns – requires significant cooperation between industry and government domestically and internationally [40].

The UN GGE report referenced above [39] recommended a number of non-political binding norms of state behaviour as well as a number of confidence, cooperative and capacity-building measures aimed at protecting critical infrastructure. Several of the eleven proposed norms are applicable to state responses to potential terrorist acts in cyberspace, including the norm that states should not knowingly allow their territory to be used for internationally wrongful acts using ICT; and the norm relating to cooperation between states as a means to 'exchange information, assist each other, prosecute terrorist and criminal use of ICT, and implement other cooperative measures to address such threats'. It also suggests that states should work together to determine whether new measures are needed in this respect.

Regarding the threat of attacks against critical infrastructure, including by terrorist groups or individuals, four of the proposed norms deal explicitly with the issue, covering prohibition against inflicting intentional damage upon critical infrastructure (CI); the state's responsibility to secure their own CI; the obligation to support other states suffering attacks on their CI; and the expectation of responsible reporting of vulnerabilities and information sharing that could prevent or mitigate cyber attacks on CI (see table 1 below).

Table 1. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174 of July 2015)

Para 13, f	A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.
Para. 13, g	States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions
Para. 13, h	States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another

	State emanating from their territory, taking into account due regard for sovereignty.
Para. 13, j	States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.

Some of these measures are already being implemented, albeit not solely within a counter-terrorism framework. Beyond intelligence sharing, today much of the international cooperation relating to the protection of critical infrastructure is centred on securing information systems, sharing information between government and industry actors, building capacity and implementing good practice.[10]

3.2 CI Protection within the Civilian Nuclear Security Sector

According to a recent Chatham House report, it was the revelation of the Stuxnet virus targeting the centrifuges of a nuclear complex in Iran, and its reported impact, that intensified concerns about intentional interference in the industrial control systems of nuclear power plants. Since, then, the report notes, there have been 'a number of reported incidents of cyber interference in nuclear power plants and – assuming that the nuclear industry behaves in similar ways to other industries – we ought to assume that these examples represent the visible part of a much more serious problem' [41]. Exploiting weaknesses in its computer systems, the report suggests, 'could be the most attractive route for those seeking to attack nuclear facilities without fear of interdiction'. This is due in part to sector regulatory requirements, and in part to tardiness in adopting digital systems and developing cyber security readiness. Nonetheless, the civilian nuclear energy sector is possibly the sector in which significant international cooperation and support in integrating computer security into nuclear security regimes at the national level is most evident.[11]

For instance, the International Atomic Energy Agency (IAEA) has established guidance for states in terms of developing a nuclear security regime as part of its 'Nuclear Security Plan for 2014–2017'. The security regime includes '[r]outinely performing assurance activities to identify and address issues and factors that may affect the capacity to provide adequate nuclear security, including cyber security, at all times' [42]. Its work addresses, *inter alia*, state and non-state sponsored attacks against civilian nuclear reactors. It also includes the possibility that 'insiders' – an important cyber security threat across all CI sectors – can represent a nuclear security threat.

The IAEA's 2011 'Technical Guidance Manual on Computer Security at Nuclear Facilities' forms part of the security regime. It notes how 'attention to computer security has intensified in the last decade as clear and recurring proof of the vulnerabilities of computer systems has come to light' [43]. Moreover, it stresses that malicious exploitation of these vulnerabilities has been witnessed with growing frequency and impact, referencing 'cyber terrorism' as a potential means of attacking a state's critical infrastructure.

---

[10] For instance, in 2013, the government of the Republic of Korea issued a technical recommendation to the management agencies of the country's public sector CII facilities which centred on separating intranet and internet physically or logically (communication with South Korean industry expert, July 2016).

[11] Communication with US and South Korean industry experts, July 2016.

Following this initial work, a number of national authorities moved to prepare defences, issuing new regulations to establish computer security requirements with implications for nuclear facilities at multiple levels and at the various stages of operation. This work intensified following the IAEA's 57th General Conference when the IAEA was encouraged to 'raise awareness of the threat of cyber attacks and their potential impact on nuclear security' and improve international cooperation [44]. The International Conference on Computer Security in a Nuclear World organised in Vienna in 2015 by the IAEA in conjunction with the ITU, INTERPOL, UNICRI and the IEC brought these efforts further. This conference was aimed at exchanging information and promoting cooperation with IAEA stakeholders, including industry actors, on the topic of computer security within the broader framework of nuclear security.

The IAEA's National Nuclear Support Administration (NNSA), which has a cyber support team, has developed a dedicated *Computer and Information Security Programme*, focused on preventing malicious computer acts at the national level that could directly or indirectly lead to unauthorised removal of nuclear or other radioactive material; sabotage against nuclear material or facilities; and theft of nuclear sensitive information. The objective of the NSNS's activities is 'to provide states with the guidance and expertise they need to develop and implement effective information and computer security to enhance their overall national nuclear security regime' [45]. The programme produces a number of technical guidance documents and organises expert meetings, training and supporting activities.

As with other sectors, a range of sector-specific, technical and cultural challenges to optimal computer and information security in this sector undoubtedly remain. Regular monitoring and reporting on how solutions to these challenges are being implemented and more frank reporting on the actual nature of 'reported attacks', would certainly help reduce uncertainty and promote cooperation and stability in this area, particularly as it relates to terrorist activity.

3.3 Critical Communications Infrastructure

Concerns have also increased with regard to potential terrorist interference with critical communications infrastructure, notably submarine fibre optic cables through which more than 95 per cent of international communications are routed and upon which the international system's reliance should not be underestimated. This reliance includes regular e-mail and telephone traffic, internet banking, e-commerce, major financial services (SWIFT etc.) as well as the critical communications capabilities and network management systems of key off shore energy installations, such as oil and gas.

It increasingly includes a number of military uses key to international and national security. For instance, and as discussed by Sechrist, a significant portion of the US Department of Defense (DoD) data travelling through undersea cables includes unmanned aerial vehicle (UAV) video, essential for war planning and prosecution [46]. In addition, the US DoD's Global Information Grid (GIG) also uses portions of the global telecoms systems, including submarine cable networks. The GIG is the 'globally, interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating and managing information on demand to war-

fighters, policy makers and support personnel', which, if interrupted by either state or non-state actors, would have important implications.

Approaching the issue from a largely economic stance, the government of Singapore has lobbied hard to highlight the level of disruption that would result from interference with these cables. A small island state with significant maritime interests, Singapore was one of the first states to realise that a single break in a submarine cable could result in huge economic costs for all the countries it connects [47]. As submarine cables are often slim and fragile, and simply laid on top of the seabed, such breaks could happen for any number of reasons, whether intentional or not.

For several years running, Singapore introduced language on submarine cables into a draft omnibus resolution on oceans and the law of the sea. In 2010 – and building on the Okinawa Declaration of an Asia Pacific Economic Cooperation Ministerial Meeting – the approved text of the Resolution in question (A/65/37A) called on member states to take measures aimed at protecting fibre optic submarine cables in accordance with commitments under the UN Convention on the Law of the Seas. It also encouraged greater dialogue and cooperation among states and the relevant regional and global organizations to promote the security of such critical communications infrastructure.

Yet, the international regime for protecting submarine cables is highly complex, and spreads across a number of different regimes covering cable protection during war-time and peace-time[12], which – due to their own complexities – do not provide full protection. Its key governance regime – the International Cable Protection Consortium (ICPC) is unique in that it is a privately run initiative (largely by multi-system operators) to which states have only been party since 2010. For some, this level of regime fragmentation (or rather dispersion) coupled with the growing threat of terrorism and state-backed interference, merits consideration of whether a dedicated treaty might be required. For Davenport, such an international instrument in the form of a treaty would make intentional interference (whether physical or via a cyber attack) with submarine cable systems an international crime and include key provisions for mutual cooperation between states on enforcement against such crimes [35]. Given the current context, however, the most likely possibility in the near-term is enhanced engagement of cable industry actors and the ICPC at the national and international levels in current discussions on cyber security and threats posed by state and non-state actors to international peace and stability.

In terms of regional arrangements, developments within the EU context relating to the protection of critical infrastructure deserve a mention. ENISA, for instance, has been supporting EU member states efforts to protect critical information infrastructure (CIIP) for some time, relying heavily on industry participation at the national and regional levels in its efforts to assist the European Commission and member states. Its most recent study 'Stocktaking, Analysis and Recommendations on the Protection of [critical information infrastructures] (CII)', provides important insights into existing and emerging risks and challenges while also show-casing a number of good practices [48]. The recommendations to national authorities and lawmakers included in the study focus on institutionalising cooperation with the private sector; harmonising CIIP

[12] International humanitarian law, including the 1907 Hague Convention for war-time; United Nations Convention on the Law of the Sea and laws of state responsibility; and, customary international law for peace time.

management structure with national crisis and emergency management structures; conducting national risk assessments; using best legal framework practices for CIIP across CI sectors; and studying how to best incentivise CII operators to invest in security measures [48].

Beyond ENISA, in July 2016 the EU adopted the Network and Information Security (NIS) Directive – also known as the 'cyber security directive' which establishes minimum obligations for all member states on the prevention and handling of, and response to, risks and incidents affecting networks, including those posed by non-state actors. It is a first attempt to legislate in the cyber security area, contrasting with the approach of other states (e.g. the US) that have opted for industry-led/voluntary approach (e.g. the sector-specific Information Sharing and Analysis Centers (ISACs), such as the Financial Security or Energy ISACs). The NIS Directive adopts a multi-layered approach by placing obligations on all stakeholders across the industry. This includes establishing minimum obligations for all member states on the prevention, handling of, and response to, risks and incidents affecting networks and information systems. It also includes a requirement of 'market operators' providing critical infrastructure, the disruption or destruction of which would have a significant impact on a member state, to comply with a mandatory security breach and incident notification requirement. In this case, market operators include operators in the energy, telecoms, banking, health, transportation and financial services sectors.[13] The NIS Directive also creates a cooperative mechanism between EU member states. Importantly, the NIS Directive also includes a paragraph reminding States of their obligations regarding respect of fundamental rights and principles enshrined in the Charter of Fundamental Rights of the EU when implementing the provisions of the Directive (para. 71). While broadly seen as a move in the right direction, many challenges remain. Hence, monitoring implementation across EU member states will be key to understanding its effectiveness, as will sharing the results of early monitoring efforts with countries in other regions.

4. Concluding Remarks

4.1 Terrorist Use of the Internet

Terrorists use the internet and ICT for strategic communications, as a powerful propaganda weapon and as an effective organizational tool for the planning, coordination and financing of their activities. The inherently transnational and multi-lingual character of this phenomenon adds to existing challenges relating to the prevention, detection and prosecution of terrorist activities. Content removal might help, as might some counter-narrative efforts, but these are hardly sustainable solutions to the structural problems affecting societies across the globe. Furthermore, in many cases such actions exacerbate existing problems, and more often than not are employed in the absence of effective integration and social and political development policies. In addition, they raise important, yet unanswered, questions about the role of different actors in global decision-making today.

[13] The telecommunications sector is already subject to incident reporting obligations, as per the EU Framework Directive.

There is no easy way around these issues. What is evident, however, is the need to engage a much broader range of actors in identifying and discussing the challenges, seeking solutions and in assessing the short and long-term effectiveness of the response and related societal implications. This becomes all the more urgent not just, as some may argue, because we are moving towards an even deeper reliance on digital tools and platforms – the so-called Internet of Things – but also because the divides in our societies are becoming deeper and more acute.

Building on existing public-private and multi-stakeholder initiatives and shaping new ones will be key. These include the aforementioned efforts led by the European Commission, as well as those being implemented under the Global Network Initiative (GNI) or the more recent UNCTED-ICT4Peace initiative focused on deepening understanding and fostering dialogue around private sector engagement in responding to terrorist use of ICT. So will determining how best to apply existing and emerging principles such as the UN 'Guiding Principles on Business and Human Rights', the European Commission's 'ICT Sector Guide on Implementing the Business and Human Rights Principles' or the Global Network Initiative's 'Principles on Freedom of Expression and Privacy'.

4.2 Terrorist Attacks Against Critical Infrastructure

There is still limited evidence that any of the terrorist groups today possess the intelligence (particularly HUMINT), capacity and capabilities to conduct the high impact disruptive cyber attacks against critical infrastructure discussed above. Yet, the vulnerabilities of existing systems mean that the risks remain and require attention.

Significant work is underway to respond to these risks, notably within the framework of the UN's First Committee on Disarmament and International Security, where agreement has been reached by government experts on a number of political norms relating to state responsibility in protecting critical infrastructure, sharing information and mutual assistance. As discussed, despite important challenges, numerous states are already implementing measures to ensure that the information systems of different critical infrastructures are safeguarded from potential attacks, whether they be conducted by terrorist groups states, or proxies, and industry actors – key to any solution – are, to a large extent, heavily engaged in such actions.

Moving forward, it will be imperative to continue strengthening public-private and multi-stakeholder cooperation and engagement in building resilience into our critical infrastructures and related information systems, responding to those legal and technical challenges to protecting critical infrastructures that have been identified, building confidence between actors within states and internationally, and ensuring that more states are included in ongoing efforts.

Finally, and as noted above, whether dealing with terrorist use of the internet or potential terrorist attacks (cyber or otherwise) against critical infrastructure, we should be wary of the increasing over-emphasis on technological solutions and ensure that counter-terrorism strategies remain equally focused on the structural issues driving people to join terrorist groups or engage in terrorist activity. An over-reliance on technology and misplaced policy has trumped strategic thinking before. It will likely do so again if we continue to act impulsively.

References

[1] *At a Glance: Understanding Definitions of Terrorism*, European Parliament, 2015.
[2] C. Kavanagh, *Information Technology and the State: The Long View*, doctoral dissertation, Department of War Studies, King's College London, 2016.
[3] Internet World Stats, http://www.internetworldstats.com/stats.htm.
[4] M. Ritchel, Egypt Cuts off Most of Internet and cell service, *New York Times*, 28 January 2011.
[5] M. Carr, *US Power and the Internet in International Relations*, Palgrave Macmillan, Basingstoke, 2016.
[6] D. Clemente, *Cyber Security and Global Interdependence: What Is Critical?*, Chatham House, London, 2013.
[7] A. Y. Zelin, al-Ḥayāt Media Center, http://jihadology.net/category/al-ḥayat-media-center/.
[8] D. Azami, The Islamic State in South and Central Asia, *Survival: Global Politics and Strategy* 58 (2016), 131-158.
[9] Brazil arrests 10 suspected ISIS members 'planning Olympic terrorist attacks', *BBC News*, 21 July 2016.
[10] *United States of America vs. Ali Shukri Amin*. 1:15-cr-164. US District Court for the Eastern District Court of Virginia, Alexandria Division.
[11] United Nations Security Council, *Report on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat* (Report S/2016/501), United Nations, New York, 2016.
[12] United Nations Security Council, *Statement by the President of the Security Council* (S/PRST/2016/6), United Nations, New York, 2016.
[13] Council of Europe, *Comparative Study of Filtering, blocking and take-down of illegal content on the Internet*, The Swiss Institute of Comparative Law, Avis 14-067, Lausanne, 2015.
[14] Article 19, Landmark European Court Decision finds blanket Google ban was a violation of freedom of expression, 18 December 2012.
[15] *Cengiz and Others v. Turkey*, European Court of Human Rights, 1 December 2015.
[16] C. Forcese and K. Roach, Limping into the Future: The U.N. 1267 Terrorism Listing Process at the Crossroads, *George Washington International Law Review* 42 (2010), 217-277.
[17] M. Wählisch, *EU Terror Listing: An Overview about Listing and Delisting Procedures*, Berghof Peace Support, 2010.
[18] T. J. Biersteker, S. Eckert and M. Tourinho (eds.), *Targeted Sanctions: The Impacts and Effectiveness of United Nations Action,* Cambridge University Press, Cambridge, 2016.
[19] United Nations Global Counter-Terrorism Strategy, 2006.
[20] M. Gercke, 10 years Convention on Cybercrime: Achievements and Failures of the Council of Europe's Instrument in the Fight against Internet-related Crimes, *Computer Law Review International* 12(5) (2011), 142–149.
[21] N. E. Marion, The Council of Europe's Cyber Crime Treaty: An exercise in Symbolic Legislation, *International Journal of Cyber Criminology* 4 (2010), 699–712.
[22] UNODC and UNCTITF, *The Use of the Internet for Terrorist Purposes*, United Nations, New York, 2012.
[23] M. Gercke, Understanding Cybercrime: A Guide for Developing Countries, International Telecommunication Union Cybercrime Legislation Resources, Geneva, 2011.
[24] E. Nakashima, Dismantling of Saudi-CIA Web Site Illustrates Need for Clearer Cyberwar Policies, *The Washington Post*, 19 March 2010.
[25] J. Lewis, *The Internet and Terrorism*. Centre for Strategic and International Studies, Washington DC, 2005.
[26] N. Muižnieks, The Rule of Law on the Internet and in the Wider Digital World, CommDH/IssuePaper (2014)1, 8 December 2014.
[27] European Commission, *Preventing Radicalisation to Terrorism and Violent Extremism: Strengthening the EU's Response*, COM(2013) 941 final, 15 January 2014.
[28] EDRi and Access Now Withdraw from the EU Commission IT Forum Discussions, EDRi, 31May 2016.
[29] Release: DIY Transparency Report Tool, Citizen Lab, University of Toronto, 30 June 2016.
[30] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, United Nations Office of the High Commissioner for Human Rights, A/HRC/32/38, 11 May 2016.
[31] 'Principles', Global Network Initiative, http://globalnetworkinitiative.org/principles/index.php.
[32] C. Kavanagh, Private Sector Engagement in Responding to the Use of the Internet and ICT for Terrorist Purposes: Strengthening Dialogue and Building Trust. (2016) UNCTED and ICT4Peace.
[33] United Nations Counter-Terrorism Implementation Task Force, *Countering the Use of the Internet for Terrorist Purposes — Legal and Technical Aspects*, United Nations, New York, 2011.

[34] E. Morozov, *To Save Everything, Click Here*, Public Affairs, New York City, 2013.
[35] T. Davenport, Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis, *Catholic University Journal of Law & Technology*. 24(1) (2015), 57-109.
[36] Website of the European Union Agency for Network and Information Security, https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services.
[37] C. Guitton and E. Korzak, The Sophistication Criterion for Attribution, *The RUSI Journal,* 158 (2013), 62-68.
[38] T. Erästö and J. Herbach, *Ten Years of the Global Initaitve to Combat Nuclear Terrorism: Strengths, Challenges and the Way Forward*, SaferGlobe, Helsinki, 2015.
[39] United Nations General Assembly, *Report of the Group of Governmental Experts On Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174, United Nations, New York, 2015.
[40] M. Carr, Public–private partnerships in national cyber-security strategies, *International Affairs*, 92 (2016), 43-62.
[41] C. Baylon, R. Brunt and D. Livingstone, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, Chatham House, London, 2015.
[42] International Atomic Energy Agency, Nuclear Security Plan 2014-2017, GOV/2013/42-GC(57)/19.
[43] International Atomic Energy Agency, *Computer Security at Nuclear Facilities*, IAEA Nuclear Security Series No. 17, IAEA, Vienna, 2011.
[44] International Atomic Energy Agency, *Resolution adopted on 20 September 2013 during the tenth plenary meeting*, GC(57)/RES/10.
[45] Donald D. Dudenhoeffer, 'Gates, Guards, Guns and Geeks: The Changing Face of Nuclear Security and the IAEA's Leading Role in Promoting Computer Security for Nuclear Facilities'. IAEA Presentation n/d.
[46] M. Sechrist, New Threats, Old Technology: Vulnerabilities in Undersea Communication Cable Network Management Systems, Discussion Paper 2012-03, Science, Technology, and Public Policy Program, Belfer Center for Science and International Affairs, Harvard Kennedy School, 2012.
[47] O. Fletcher and J. Osawa, Rush to Fix Quake-Damaged Undersea Cables, *The Wall Street Journal*, 15 March 2011.
[48] S. Anna and M. Konstantinos, *Stocktaking, Analysis and Recommendations on the Protection of CIIs*, ENISA, Heraklion, 2016.