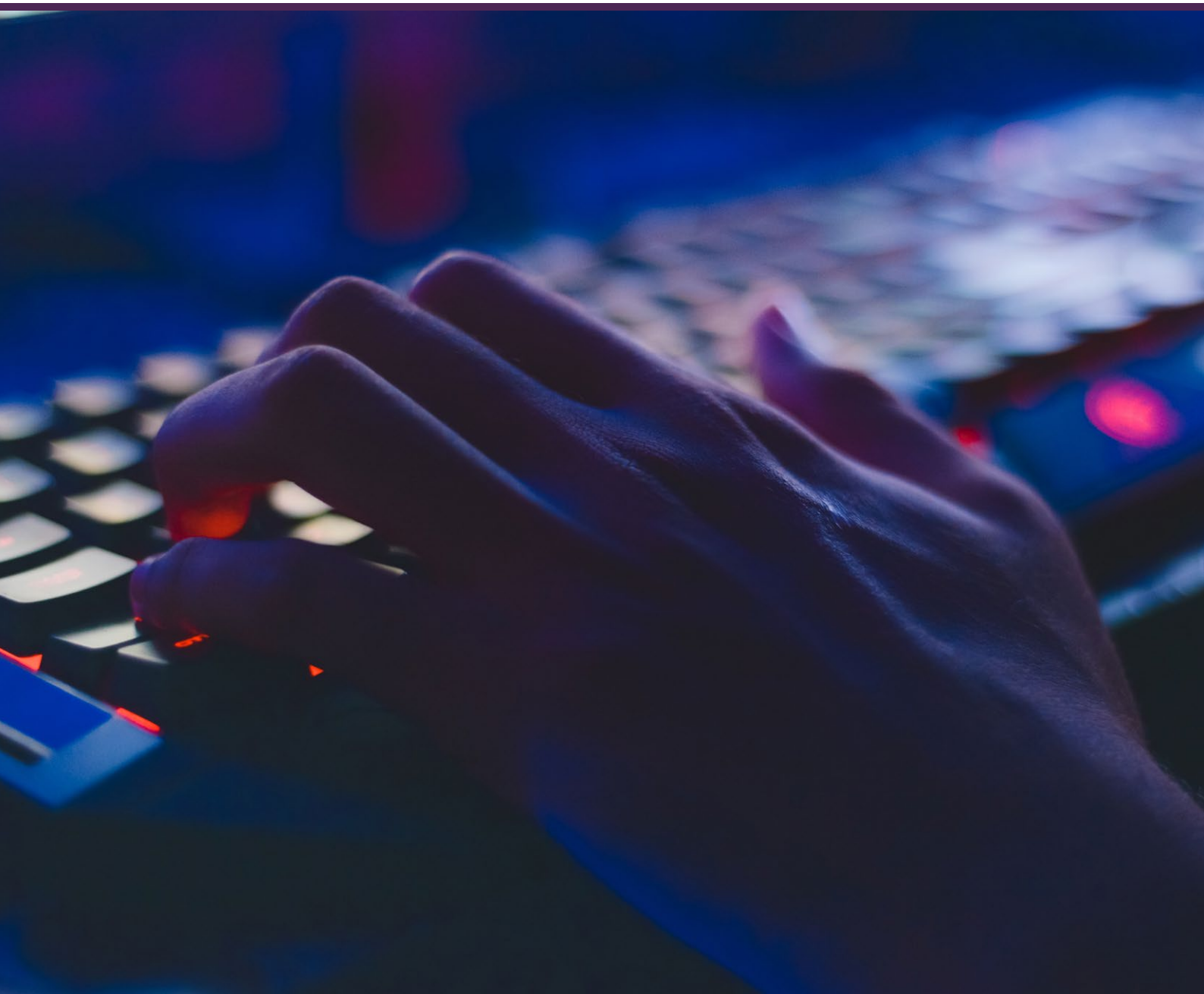
RUSI
www.rusi.org
Royal United Services Institute
for Defence and Security Studies

IDC HERZLIYA 25
ICT International Institute for Counter-Terrorism
With the Support of Keren Danie

Global Research Network on Terrorism and Technology: Paper No. 9

The International Cyber Terrorism Regulation Project

Deborah Housen-Couriel, Boaz Ganor, Uri Ben Yaakov,
Stevie Weinberg and Dafne Beri



The International Cyber Terrorism Regulation Project (ICTRP) has established an online resource consisting of a compilation of online regulatory resources in the field of counterterrorism, and an analytical framework for their use. This paper provides an overview of the project, which is funded by the Global Research Network on Terrorism and Technology.

The ICTRP provides an initial mapping of 16 state and non-state actors (countries, international organisations and social media providers) that employ regulatory measures for online counterterrorism. Based on this initial analysis, the research has identified key areas for cooperation among these actors and provides five specific recommendations for moving ahead in each area. Space limitations preclude inclusion of the research methodology section of the project in this paper; it may be found, together with other materials, on the ICTRP website (https://www.ictrp.org/).

The present ICTRP research has three primary aims:

1. To identify key areas for cooperation in bolstering online counterterrorism among the 16 stakeholders studied.
2. To carry out an initial mapping of these stakeholders' increasingly diverse regulatory measures (including laws, strategies, policies, treaties, multilateral resolutions and capacity-building initiatives).
3. To facilitate key areas for cooperation among stakeholders by compiling these measures via the ICTRP website, and proposing a methodology for highlighting their similarities and differences.

These aims are supported by the analytical framework developed for 'disaggregation' of these regulatory measures across 10 major categories of terrorist use of the internet.

Key Findings

Currently, the regulatory measures studied are characterised by several challenges to enhancing cooperation and effectiveness among stakeholders, including:

- A lack of common definitions of prohibited terrorist internet activity across jurisdictional lines and within jurisdictions for different social media platforms (SMPs).
- The absence in most national jurisdictions of an overarching conceptual and strategic approach to counterterrorism on the internet.
- The development of autonomous corporate policies and measures by those SMPs that are also multinational corporations, which may differ between jurisdictions.

Recommendations

- Effective counterterrorism cooperation requires a multidimensional, multi-stakeholder approach that is not only tactical, but also strategic.
- Small and medium-sized SMPs should be provided with tools and capacity-building measures, including tailored training exercises and 'how-to' guides.
- Diverse modes of information sharing of regulatory measures and practices should be implemented. The ICTRP website, which is one outcome of the research, may serve as an example of a platform for transparent and trusted information exchange.
- All stakeholders should optimise joint use of technological tools that aid in countering terrorist abuse of the internet, with appropriate oversight and rule of law constraints.
- Further attention should be given to regulation and multi-stakeholder cooperation regarding terrorist abuse of the internet that results in physical destruction and damage, including the loss of life (acts of cyber terrorism per se). The potential damage of what may be currently characterised as a 'black swan event' demands the attention of regulators and, indeed, all stakeholders engaged with online and physical-world counterterrorism.

Background

Thirty years after the invention of the Web, more than half of humanity is connected to this shared resource, contributing dramatically to the ease and speed with which many, perhaps most, human activities can be accomplished and potentially shared with a global audience. On the other hand, these advantages have been increasingly clouded by the exploitation and misuse of the internet by criminals and terrorists. In light of these new threat vectors, countries, international organisations and SMPs are engaged in an ongoing process to develop regulatory measures that specifically address counterterrorism responses to terrorist use of the internet. This global process has some common, transjurisdictional elements, but still lacks an optimal, strategic approach that fully leverages common understandings, insights and capabilities.

The scope of the ICTRP encompasses the initial mapping of the 16 state and non-state actors analysed, and on the basis of that initial mapping the identification of key areas for cooperation among them. This should be understood as the first stage in a project with broadened scope anticipated that will allow resources for a full comparative legal and regulatory analysis of the initiatives that have been mapped. This full analysis will allow more in-depth conclusions and refinement of recommended measures for concrete steps to facilitate cooperation among counterterrorism stakeholders. The ICTRP website provides access to the materials used in this first stage, including references and links to sources.

The research for this paper, including the ICTRP website which serves as its basis (www.ictrp.org), presents the stakeholders' diverse regulatory measures to counter the use of the internet by terrorists to provide an initial identification of the key areas for cooperation among these stakeholders, to increase accessibility to this information, and to provide a clear classification and methodology for its analysis and use. Such multi-stakeholder, global cooperation is critical because the internet is borderless. Closer interaction and cooperation between all stakeholders, both governmental and private sector, is needed to be optimally effective across jurisdictions, whether organisational, regional, international, national or domestic, or within SMPs that provide transboundary services. Such interactions may focus around dedicated centres for joint law enforcement (such as Interpol's Counter-Terrorism Fusion Centre, which works to disrupt the recruitment and activities of foreign terrorist fighters), ongoing forums for practitioners, and joint training exercises.

Yet at the crux of such cooperation is the regulatory and policy context studied in this paper, which includes stakeholders' counterterrorism strategies, policies, laws, and enforcement measures.[1] The ICTRP project has identified that existing regulations and policy suffer from three main challenges:[2]

1. See, for example, Interpol, 'UN Global Counter-Terrorism Strategy: Summary', February 2017, <https://www.un.org/counterterrorism/ctitf/en/un-global-counter-terrorism-strategy>, accessed 17 July 2019; the UN Office of Counter-Terrorism annexed Plan of Action of 2006, which specifically addresses 'terrorism in all its forms and manifestations on the Internet', <https://www.un.org/counterterrorism/ctitf/en/un-global-counter-terrorism-strategy#plan>, accessed 17 July 2019; Council of the European Union, 'Council Directive 2017/541 of the European Parliament and of the Council of 15 March 2017 on Combating Terrorism and Replacing Council Framework Decision 2002/475/JHA and Amending Council Decision 2005/671/JHA', *Official Journal of the European Union* (L88/6, 31 March 2017); European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on Preventing the Dissemination of Terrorist Content Online: A Contribution from the European Commission to the Leaders' Meeting in Salzburg on 19-20 September 2018', COM(2018) 640 final, 12 September 2018.
2. The ICTRP has mapped and analysed the regulatory measures undertaken in five countries (France, Germany, Israel, the UK and the US); in six international organisations (the EU, Europol, Interpol, NATO, the OSCE and the UN); and in five SMPs that operate globally (Facebook, Google, Microsoft, Twitter and YouTube). For full details, see the project website at www.ictrp.org.

1. There exists a lack of common definitions of prohibited terrorist internet activity, which can impede optimal enforcement across jurisdictional lines and within jurisdictions for different SMPs.[3]
2. Despite the significant number of existing counterterrorism strategies and policies with respect to terrorist abuse of the internet, most national jurisdictions have yet to develop an overarching conceptual and strategic approach to counterterrorism on the internet across their own regulatory measures relating to the 10 categories analysed, and to support this chosen approach with educational, media and other societal initiatives.
3. Multinational SMPs have developed autonomous corporate policies and measures that are likely to differ from national jurisdictions. Such policies work to address terrorist activity on the internet, such as the spread of propaganda and incitement.[4] These large SMPs have made robust progress in this context within the specific scope of terrorist content.[5] Yet such measures, as they develop, still need to close some gaps. To note just four of these, for example: 1. They are not necessarily fully coordinated with one another, even where specific tailoring to different operational and business models is appropriate; 2. Small and medium-sized SMPs may not be coordinated with these initiatives, nor are they always aware of the need to coordinate; 3. SMP efforts may not be optimally engaged with national and transnational enforcement mechanisms (such as Interpol and Europol); and 4. SMPs are not bound by the regulatory oversight processes that constrain the activities of governmental regulators in democratic societies.[6] A particular challenge that has been identified within the SMP stakeholder community is the gap between policies currently implemented by large, global SMPs that have internal organisational capacity to develop and implement counterterrorism measures, and small and medium-sized SMPs that currently do not.

---

3. This is similar to the well-known policy challenge of defining 'terrorism' and overlaps with the issue of categorising illicit activities as 'criminal' or 'terrorist'.
4. See, for example, YouTube, 'Violent or Graphic Content Policies, <https://support.google.com/youtube/answer/2802008?hl=en>, accessed 21 July 2019.
5. See, for example, YouTube, 'Official Blog: Our Ongoing Work to Tackle Hate', 5 June 2019, <https://youtube.googleblog.com/2019/06/our-ongoing-work-to-tackle-hate.html?m=1>, accessed 12 June 2019.
6. See, for example, Twitter, 'Terrorism and Violent Extremism Policy: Overview', March 2019, <https://help.twitter.com/en/rules-and-policies/violent-groups>, accessed 21 July 2019.

Meeting these three challenges is a difficult task at the aforementioned level of inter-jurisdictional, multi-stakeholder coordination. Moreover, beyond the issue of coordination, several key substantive policy issues are difficult to resolve. For example, one of the core issues for providing an effective response to terrorist use of the internet in democratic, rule of law countries is to find a balance between national security needs and basic human rights, such as freedom of speech, within the applicable law in each jurisdiction.[7] It is critical to address this and other key dilemmas associated with the implementation of evolving counterterrorism policies and strategies, both at the national and transnational levels.

An additional challenge, addressed by some of the existing policies and regulations, that requires multi-stakeholder attention and cooperation is terrorist abuse of the internet that results in physical destruction and damage, including the loss of life (acts of cyber terrorism per se within the ICTRP methodology). Several points are salient. On the one hand, such acts of cyber terrorism have not yet taken place or have not been transparently attributed to terrorist organisations. Terrorist groups may not yet possess the requisite capabilities to inflict such damage. On the other hand, such capabilities are available for purchase or for use by terrorist organisations as state proxies. The potential damage of what may be currently characterised as a 'black swan event' demands the attention of regulators and, indeed all stakeholders engaged with online and physical-world counterterrorism. The foiled attempt by Gaza-based Hamas terrorists to inflict damage on Israel's infrastructure in May 2019 gives a strong indication that physical damage inflicted by cyber-enabled acts of terror is just a matter of time.[8]

Existing Policies and Types of Regulators

Terrorists increasingly leverage their use of the internet for malicious purposes. The ICTRP identifies 10 major categories of hostile activity: propaganda; psychological operations; incitement; recruitment; radicalisation; financing;

7. As noted in the 2016 Report on the Implementation of the UN Global Counter-Terrorism Strategy: 'The importance of protecting an individual's right to freedom of expression has to be balanced with the need to protect a vulnerable audience from incitement to hatred, discrimination or violence'. See UN General Assembly, 'Activities of the United Nations System in Implementing the United Nations Global Counter-Terrorism Strategy', A/70/826, 12 April 2016, p. 4, <https://www.ictrp.org/wp-content/uploads/2019/02/Activities-of-the-United-Nations-system-in-implementing-the-United-Nations-Global-Counter-Terrorism-Strategy-2016.pdf>, accessed 21 July 2019.
8. Kate O'Flaherty, 'Israel Retaliates to a Cyber-Attack with Immediate Physical Action in a World First', *Forbes*, 6 May 2019, <https://www.forbes.com/sites/kateoflahertyuk/2019/05/06/israel-retaliates-to-a-cyber-attack-with-immediate-physical-action-in-a-world-first/#4f2676c8f895>, accessed 21 July 2019.

information sharing; intelligence; communications; and cyber terrorism (see below for an explanation of these categories). At the same time, governments and international organisations are developing measures to fight and mitigate such abuses of the internet with an increasingly diverse regulatory toolbox, including laws, strategies, policies, treaties, multilateral resolutions, and capacity-building initiatives. In addition, this regulatory toolbox increasingly includes policies and measures initiated by key SMPs and applied by them autonomously to monitor and remove terrorist content and to block other internet-enabled terrorist activities.

The ICTRP website includes an overview of existing regulations in 16 selected stakeholders, which have been chosen for the diversity of regulatory measures they employ, as well as for the degree of cooperation which already exists between some of them. Each applies regulatory measures to terrorist abuse of the internet, and they have been divided into three categories: countries (France, Germany, Israel, the UK and the US); international organisations (Europol, the EU, Interpol, NATO, the OSCE and the UN), and SMPs (Facebook, Google, Microsoft, Twitter and YouTube). This diversity might be expanded to encompass an even broader scope of measures and geographical distribution.

Countries

Countries traditionally regulate counterterrorism measures through national strategies, laws and policies. These measures have effect within jurisdictional boundaries and are enforced through national policing and security authorities that are both defined by law, and subject to judicial review of their activities. The countries reviewed for the ICTRP represent a diversity of approaches to defining terrorist activity on the internet, to regulating its illegality, and to establishing enforcement powers to mitigate its impact. Some countries address terrorist activity online separately from such activity in the physical world, and others do not make such a separation. Israel's Counter-Terrorism Law of 2016, for example, adopts a unified approach that categorises illegal activity as an act of terrorism according to its end result.[9] In the context of enforcement measures, several countries, such as France and the UK, have made strides in engaging the public to identify terrorist content and other terrorist activity online. Examples of these include the French website Stop-Djihadisme, http://www.stop-djihadisme.gouv.fr/, and the UK website https://www.gov.uk/report-terrorism, which provide mechanisms for the reporting of terrorist content and activities that potentially violate national laws. Such mechanisms represent a feasible regulatory measure

9. Library of Congress, 'Israel: New Comprehensive Counterterrorism Legislation Adopted', Global Legal Monitor, <https://www.loc.gov/law/foreign-news/article/israel-new-comprehensive-counterterrorism-legislation-adopted/>, accessed 17 July 2019.

which may be easily reproduced and coordinated between countries, international organisations and SMPs.

International Organisations

The international organisations reviewed in the ICTRP also approach the counterterrorism challenges of terrorist use of the internet through a variety of regulatory tools. These include multilateral agreements and arrangements, such as the EU's March 2017 Directive on Combating Terrorism, including terrorist use of the internet, and the proposed Regulation of September 2018 on preventing the dissemination of terrorist content online;[10] as well as white papers such as the OSCE's counterterrorism commitments of 2018[11]. In addition, international organisations such as Interpol and Europol have dedicated resources and capacity-building to the fight against online terrorism activities and the enforcement of regulatory measures. One example is Interpol's Counter-Terrorism Fusion Centre which focuses on terrorist use of SMPs. Such organisational mechanisms for coordinating multi-stakeholder responses are critical and represent important opportunities for bolstering cooperation across jurisdictions. This is one example of the important role of international organisations in setting transnational, multilateral definitions of terrorist activity in cyberspace, legal and practical norms for combating illicit terrorist activity online beyond national borders, and modes of cooperation for bolstering law enforcement globally.

SMPs

The use of SMPs by terrorist groups to promote their ideologies, distribute propaganda and incitement, recruit operatives and collect funds is now an urgent, critical issue for all stakeholders, including transnational enforcement agencies such as Interpol and Europol.[12] Governments may undertake regulatory and enforcement initiatives, including judicial or administrative takedown orders for terrorist content on SMPs. SMPs publish policies for their users that specifically define the types of terrorist content or other

10. Council of the European Union, 'Council Directive 2017/541 of the European Parliament and of the Council of 15 March 2017 on Combating Terrorism and Replacing Council Framework Decision 2002/475/JHA and Amending Council Decision 2005/671/JHA'; European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on Preventing the Dissemination of Terrorist Content Online'.
11. OSCE, 'Overview of OSCE Counter-Terrorism Related Commitments', SEC.GAL/69/18, 19 April 2018, <https://www.osce.org/node/26365?download=true>, accessed 21 July 2019.
12. Sheera Frenkel and Ben Hubbard, 'After Social Media Bans, Militant Groups Found Ways to Remain', *New York Times*, 19 April 2019; Muddassar Ahmed, 'Opinion: Facebook Needs to Crack Down on Hate Speech. So Does Mainstream Media', *BuzzFeed News*, 10 April 2019.

online activity that will result in a prompt investigation and eventual removal from their platforms. This process may be supported by artificial intelligence and machine learning programmes that identify and remove such content, in addition to human staff who review and escalate removal requests. Three examples are: YouTube's Community Guidelines, which include a flagging feature for users to note problematic content;[13] Facebook's Community Standards Guidelines that define 'dangerous individuals and organizations', including a terrorist and terrorist organisations;[14] and Twitter's policy prohibiting violent threats and the glorification of violence, including terrorist acts.[15] These policies are currently undergoing significant re-evaluation, as new challenges to SMPs with respect to online terrorist activity continue to develop.[16]

Common SMP definitions of prohibited terrorist content and terrorist abuse of the internet have become critical, including their substantive connection to the national definitions referred to above, as well as common standards and practices for both tactical (real-time) and strategic enforcement in concert with countries and international organisations.

Methodology

The methodology for this research has been adapted to the scope of the project, which is limited to identifying key areas of cooperation among counterterrorism stakeholders on the basis of the mapping of regulatory measures described above. This methodology classifies the means by which terrorists abuse the internet into 10 categories: propaganda; psychological operations; incitement; recruitment; radicalisation; financing; information sharing; intelligence; communications; and cyber terrorism.[17] These categories are based on the 2012 UN Office on Drugs and Crime report, 'The Use of the Internet for Terrorist Purposes', which identifies six categories: propaganda (including recruitment, radicalisation and incitement to terrorism); financing; training; planning (including through secret communication and open-source information); execution; and cyber attacks.[18] This basis was adapted to the

13. YouTube, 'Policies and Safety', <https://www.youtube.com/intl/en-GB/yt/about/policies/#community-guidelines>, accessed 17 July 2019.
14. Facebook, 'Community Standards', <https://en-gb.facebook.com/communitystandards>, accessed 17 July 2019.
15. Twitter, 'The Twitter Rules', <https://help.twitter.com/en/rules-and-policies/twitter-rules>, accessed 17 July 2019.
16. For example, see the references to online terrorist activity in Mark Zuckerberg, 'The Internet Needs New Rules: Let's Start in These Four Areas', *Washington Post*, 30 March 2019.
17. See https://www.ictrp.org/terrorist-use-of-the-internet/ for detailed information on each of these categories.
18. UN Office on Drugs and Crime, 'The Use of the Internet for Terrorist Purposes', September 2012.

10 categories included in the ICTRP after conducting several discussions with ICT experts and the authors' own expertise. There is a certain degree of inevitable overlap among these categories.

By comparing how regulations and policies in each of the selected countries and organisations address the aforementioned categories, the analysis supports two separate sets of initial findings: 1) an overall mapping of the existing policy situation in each jurisdiction or organisation; and 2) a cross-section of the treatment of each of the 10 categories of terrorist abuse of the internet by the jurisdictions and organisations studied. Thus, for example, the treatment of incitement, recruitment and financing may be compared across jurisdictional and organisational boundaries.[19] Through applying such an analytical matrix, which needs to be fully developed, multi-stakeholder cooperation for counterterrorism may become more focused, transparent and ultimately effective – and may more readily include small and medium-sized SMPs.

19. See Annexes 2 and 3 in the methodology section of the ICTRP website for existing laws and strategies, respectively, <https://www.ictrp.org/about-ictrp/>.

Recommendations

Below are several recommendations that flow from the ICTRP research carried out so far. Prioritisation of their implementation through cooperative initiatives is a separate issue for analysis, entailing discussion of resources and the leveraging of cooperation mechanisms already in place, such as Interpol's Counter-Terrorism Fusion Centre.

The focus is on key areas where there is a high potential for strengthening counterterrorism cooperation and enabling shared action and cooperation in the categories in which they are most likely to bear fruit. It is important to continue to identify which of the 10 categories already have commonalities, and to develop a model toolkit of strategy, policy and enforcement measures for each category. An important first step is to move ahead with agreement in principle on the definitions of illegal terrorist activity online – even if these are, de facto, working definitions rather than official legal definitions. The initial research carried out by ICTRP on the latter will serve as a starting point for the next stage of research.

1. Emphasise multi-stakeholder engagement. To ensure effective national and international counterterrorism cooperation for countering terrorist abuse of the internet, it is critical for state and non-state actors to engage with a multidimensional, multi-stakeholder approach that is not only tactical, but also strategic. One specific example of such engagement is convening and training key personnel within the counterterrorism ecosystem, bringing together police, counterterrorism experts and practitioners, policymakers, ICT experts, lawmakers, social-media experts, and others for meetings, focused education sessions and debate on specific, practical issues.
2. Within the multi-stakeholder paradigm, focus on providing small and medium-sized SMPs with tools and capacity-building measures to implement policies to counter terrorist use of the internet. Such tools and measures may include 'how-to' guides, self-examination of a checklist of essential measures, and similar.
3. Implement diverse modes of information sharing on regulatory measures and practices. Much more information exchange is needed on the range of different regulatory tools available to all stakeholders (laws, policies, strategies, informal arrangements, codes of conduct, bilateral agreements, citizen education and online awareness). The ICTRP website exemplifies this type of platform, which should be continually updated and adapted to stakeholder needs.
4. Further joint use and development of technological tools. Within rule of law constraints and with appropriate oversight, use technological measures to track and attribute terrorist activities online.
5. More emphasis should be put on developing measures and tools for countering potential cyber attacks by terrorists, due to this

category's high potential for loss of human life and direct physical damage, together with the increasing possibility of such cyber attacks occurring on the basis of their own developing capacities or ability to leverage the readily available capacities of other hostile actors.

Annexes

Annex 1: Taxonomy of Terrorist Use of the Internet

Annex 2: Existing Laws Regarding Terrorist Use of the Internet

Annex 3: Existing Strategies and Policies Regarding Terrorist Use of the Internet

The full annexes of the paper are available at: https://www.ictrp.org/wp-content/uploads/2019/07/Please-find-here-the-full-annex-of-the-policy-paper.pdf

Deborah Housen-Couriel is a Research Associate at the International Institute for Counter-Terrorism (ICT) and an Adjunct Professor at the Interdisciplinary Center (IDC), Herzliya, Israel.

Boaz Ganor is the Founder and Executive Director of the International Institute for Counter-Terrorism (ICT). He also serves as the Dean and Ronald S Lauder Chair in Counter-Terrorism of the Lauder School of Government, Diplomacy and Strategy at the Interdisciplinary Center (IDC), Herzliya, Israel.

Uri Ben Yaakov is the Director of Development and a Senior Researcher at the International Institute for Counter-Terrorism (ICT) at the Interdisciplinary Center (IDC), Herzliya, Israel.

Stevie Weinberg is the Deputy Executive Director of the International Institute for Counter-Terrorism (ICT) at the Interdisciplinary Center (IDC), Herzliya, Israel.

Dafne Beri is a Researcher and Project Coordinator at the International Institute for Counter-Terrorism (ICT) at the Interdisciplinary Center (IDC), Herzliya, Israel.

The authors would like to thank the group of expert peer reviewers who assisted with the initial stage of research. The full list of these experts appears on the ICTRP website.

About RUSI

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 188 years.

About The Global Research Network on Terrorism and Technology

The Global Research Network on Terrorism and Technology is a consortium of academic institutions and think tanks that conducts research and shares views on online terrorist content; recruiting tactics terrorists use online; the ethics and laws surrounding terrorist content moderation; public–private partnerships to address the issue; and the resources tech companies need to adequately and responsibly remove terrorist content from their platforms.

Each publication is part of a series of papers released by the network on terrorism and technology. The research conducted by this network will seek to better understand radicalisation, recruitment and the myriad of ways terrorist entities use the digital space.

The network is led by the Royal United Services Institute (RUSI) in the UK and brings together partners from around the world, including the Brookings Institution (US), the International Centre for Counter-Terrorism (Netherlands), Swansea University (UK), the Observer Research Foundation (India), the International Institute for Counter-Terrorism (Israel), and the Institute for Policy Analysis of Conflict (Indonesia).

The research network is supported by the Global Internet Forum to Counter Terrorism (GIFCT). For more information about GIFCT, please visit https://gifct.org/.

The views expressed in this publication are those of the authors, and do not reflect the views of RUSI or any other institution.

Published in 2019 by the Royal United Services Institute for Defence and Security Studies.

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org

RUSI is a registered charity (No. 210639)