Countering cyber terrorism in a time of 'war on words' Kryptonite for the protection of digital rights?

Edited by Fabio Cristiano, Dennis Broeders, and Daan Weggemans

THE HAGUE PROGRAM for Cyber Norms

Universiteit Leiden

Table of contents

Suggested citation:
Cristiano, F., D. Broeders and D. Weggemans (eds.) (2020). *Countering cyber terrorism in a time of 'war on words': Kryptonite for the protection of digital rights?* The Hague: The Hague Program for Cyber Norms. October 2020.

ISBN: 9789083109596
e-ISBN: 9789083109503

1. Introduction: cyber terrorism and human rights from the national to the international, and back?

Fabio Cristiano, Dennis Broeders, and Daan Weggemans

Cyber terrorism: the controversial nature of a (non) phenomenon?

Already in 1991, the US National Academy of Sciences prophesied that 'tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb'.[1] Thirty years on, this prediction has not materialized, but has been kept alive in the diplomatic language of international cyber security and across national security legislations. Where do these actors draw the boundaries of cyber terrorism? How do these get enacted in national security contexts? At what potential costs for individual and collective freedoms?

Often abused in public discourse to refer to all sorts of cyber offensive activities,[2] the conceptual boundaries of cyber terrorism remain debated and open to different interpretations.[3] This unclarity pertains, above all, to whether cyber terrorism exclusively covers violent cyber operations conducted by terrorist groups, or also includes non-violent terrorist activities: training, planning, funding, recruitment, and incitement.[4] Drawing the boundaries of the phenomenon primarily defines whether actual instances of cyber terrorism have ever occurred, and thus whether policy applications need to address a 'possible' or a 'probable' reality.[5] Unravelling the contested nature of this phenomenon is more than just an academic exercise in pursuit of conceptual clarity. Rather, exploring the definitional nuances of the concept is vital to reflect on type, extent, proportionality, and temporality of relevant national security responses, as these tend to impact fundamental liberties, both online and offline.[6]

Cyber terrorism constitutes an important issue across the different parts of the UN ecosystem, surfacing in the first (international security, UN GGE and OEWG) and third committee (cybercrime). In the first committee, two diplomatic processes promoting responsible state behavior in cyberspace through international law, shared norms, and other measures may address cyber terrorism.

1 National Research Council. *Computers at Risk: Safe Computing in the Information Age*. The National Academies Press, Washington, DC, 1991.

2 Jarvis, Lee, Stuart Macdonald, and Andrew Whiting. "Unpacking cyberterrorism discourse: Specificity, status, and scale in news media constructions of threat", *European Journal of International Security* 2, no. 1 (2017): 64-87.

3 Jarvis, Lee, and Stuart Macdonald. "What is cyberterrorism? Findings from a survey of researchers", *Terrorism and Political Violence* 27, no. 4 (2015): 657-678.

4 Conway, Maura. "Reality check: assessing the (un) likelihood of cyberterrorism", in *Cyberterrorism*, pp. 103-121. Springer, New York, NY, 2014.

5 Stevens, Tim. "Strategic cyberterrorism: problems of ends, ways and means", in *Handbook of Terrorism and Counter Terrorism Post 9/11,* pp. 42-52. Edward Elgar Publishing, 2019; and Aradau, Claudia, and Rens Van Munster. "The time/space of preparedness: Anticipating the "next terrorist attack"", *Space and Culture* 15, no. 2 (2012): 98-109.

6 Heinl, Caitriona. "Terrorist access to offensive cyber means and how this threat might be best managed". In the *Oxford Handbook of Cyber Security.* Oxford University Press, forthcoming.

Throughout its mandate, the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) has consistently engrained the possibility of cyber terrorism in its consensus reports (2010, 2013, and 2015), in both the threat section and in the policy recommendation sections of the reports. The 2015 report states that 'the use of ICTs for terrorist purposes – *beyond* recruitment, financing, training and incitement – including terrorist attacks against ICTs or ICT – dependent infrastructure, is an increasing possibility that, if left unaddressed, may threaten international peace and security' [emphasis added].[7] In 2017, after years of constructive cooperation on the issue of responsible state behavior in cyberspace, the GGE was unable to reach consensus on a final report, revealing the polarized and politicized dynamics of the process.[8]

This pause turned into a split process: in 2018, the UN General Assembly approved both an American-backed resolution 'renewing' the mandate of the GGE, as well as a Russian one establishing the Open-Ended Working Group (OEWG).[9] Negotiations are ongoing for both processes at the time of writing. At the OEWG – a more transparent process than the UN GGE which deliberates behind 'closed doors' – the language of (cyber-) terrorism has already surfaced as an item of international cyber security. The recent OEWG's chair pre-draft of the final report – to be negotiated by member states towards consensus in the near future – stresses that 'non-State actors have demonstrated ICT capabilities previously only available to States, and concern was expressed that these capabilities could be used for terrorist or criminal purposes'.[10]

Notwithstanding the fact that there are real dangers out there in terms of the terrorist use of ICTs, the international diplomatic language plays an important role in mediating and legitimizing national policy developments. After all, diplomatic processes such as those of the GGE and the OEWG are also about uploading and negotiating national policy positions. In this light, it is important to understand how the international and the national language on cyber terrorism interplay. With the aim of unraveling and problematizing this interplay, this collection of essays investigates (a) how states or regional organizations define and enact cyber terrorism and counter terrorism, and (b) to what extent these legislations undermine human and digital rights for populations that are targeted, and may or may not be legitimately considered (cyber) terrorists.

This collection includes six short policy-focused contributions exploring how legislation and policy on counter cyber terrorism unfold at the national level in the United States, the United Kingdom, China, Russia, France, and at the regional level of the European Union. The selection of the five permanent members (P5) of the United Nations Security Council as case studies stems from the recognition of their role as prominent normative actors of international cyber security. Additionally, these cases

7 United Nations. *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, New York, NY, 2015.

8 Cfr. Cristiano, Fabio. "The Road Toward Agonistic Pluralism for International Cyber Norms", *Net Politics,* Council on Foreign Relations, New York, July 2020.

9 Cfr. Broeders, Dennis and Bibi van den Berg. "Governing Cyberspace. Behavior, Power, and Diplomacy", in *Governing Cyberspace. Behavior, Power, and Diplomacy,* pp. 1-15. Rowman and Littlefield, London, 2020.

10 United Nations. *Second "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security*. New York, NY, 2020.

are also representative of the different, and strongly opposed, narratives at play.[11] In addition to these national snapshots, the case of the European Union has been included because it offers the possibility to reflect on the 'regional' level, as well as to widen the analysis to an increasingly important normative actor for coordinated counter terrorism policy.[12] Each of these contributions tackles the following questions: do national security legislations explicitly refer to cyber terrorism?; what are the boundaries set for the phenomenon?; in which situations does this framework get enacted?; what is the relationship between counter terrorism legislation and other legislation on the cyber element?

Human and digital rights between the national and the international

The possibility of cyber terrorism as low-possibility/high-consequence event has justified, from the war on terror onwards, the adoption of pre-emptive security measures through the 'spreading' of cyber security legislations across different policy domains.[13] As argued by Huszti-Orban in Chapter 2, the United States' Patriot Act (2001) set the foundations for this approach, by merging the governance of national security with defense and intelligence, while distancing itself from international standards. As shown in Chapter 3 by Mott, the construction of the cyber terrorist's threat similarly continues to permeate United Kingdom's different national policies dealing with cyberspace.

In the wake of a recent wave of terrorist attacks in Europe, and in particular in response to the online threats posed by the Islamic State (IS), western countries have developed counter-terrorism strategies for cyberspace that primarily focus on online behaviors related to preparatory and supporting activities for cyber terrorism.[14] By doing so, the national policy interest has further shifted from destructive cyber terrorism to other terrorist activities in cyberspace – that is from effects to intents.

For their reliance on intrusive surveillance, these legislations have been criticized for the impact they have on digital rights such as freedom of speech, right to internet access, net neutrality, right to privacy, and more. In particular, for the focus on online contents and their moderation, they intersect with what many believe to be the new phase of the war on terror: the 'war on words'.[15] Several recent UN initiatives – such as the works of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism and the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression – have highlighted the importance of human and digital rights standards when developing national counter-terrorism strategies for cyberspace.[16]

11 Whereas liberal countries (the so-called 'like-minded') favor a cooperative and rules-based governance under a multi-stakeholder model for international cyber security, other countries – lead by Russia and China – are advocates of 'cyber sovereignty', i.e. the ability of states to act independently on matters related to the security of their national cyberspace, and favor multilateral governance structures.

12 Cfr. Lațici, Tania. "Understanding the EU's approach to cyber diplomacy and cyber defence", European Parliamentary Research Service (EPRS), Brussels, 28 May 2020.

13 On the ideological impact this has on cyber security, see Hansen, Lene and Helen Nissenbaum. "Digital disaster, cyber security, and the Copenhagen School", *International studies quarterly* 53/4 (2009): 1155-1175.

14 For this reason, countries targeted by these attacks – France above all – have been the driving force behind this shift in policy focus, both nationally, regionally, and internationally.

15 Walker, Clive. "The war of words with terrorism: an assessment of three approaches to pursue and prevent", *Journal of Conflict and Security Law* 22/3 (2017): 523-551.

16 In particular, please see the following thematic reports: Report on online hate speech (2019, A/74/486); Report on content regulation (2018, A/HRC/38/35); and the Report on the adverse effect of the surveillance industry on freedom of expression (2019, A/HRC/41/35).

International diplomatic initiatives on cyber norms – UN OEWG and UN GGE – also increasingly discuss the importance of human rights in the context of international cyber security, somewhat broadening their normative horizons beyond the scopes of the UN First Committee. As stated in the opening paragraph of the OEWG's pre-draft, "developments in ICTs have implications for all three pillars of the United Nations' work: peace and security, human rights and sustainable development".[17]

This recognition pertains to the understanding of international cyber security as a multi-faceted phenomenon, to be addressed through complementarity and regular institutional dialogue amongst specialized UN bodies, and beyond.[18] The OEWG pre-draft's auspice that 'norms of responsible State behavior are consistent the promotion of human rights' has received contrasting national responses at the OEWG.[19] On the one hand, like-minded countries welcomed the broadening of the draft's scope towards human rights, and in fact argued for this element to be more prominent.[20] On the other hand, a number of countries – led by Russia and China – oppose this language in the context of the OEWG and the UN GGE.[21]

With the issue of human rights somewhat polarizing the debate at the UN OEWG, a growing 'coalition of the unwilling'[22] seems increasingly favorable to the inclusion of terrorism in the international diplomatic language on cyber security. As shown in Parkin's contribution (chapter 4), Chinese authorities increasingly embrace the language of counter terrorism in their strategy for information security, stretching the terrorist 'label' as to include the so-called 'three evils' of cyberspace: terrorism, extremism, and separatism. This stretching of counter terrorism has been already employed to persecute political movements as well as religious and ethnic minorities for contents posted online.[23] Through an analogous approach to national cyber security, Russia similarly leverages on the narrative of cyber terrorism to implement its centralizing strategy for information

17 United Nations. *Second "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security*. New York, NY, 2020.

18 See background paper issued by the Chair of the OEWG, "An Initial Overview of UN System Actors, Processes and Activities on ICT-related issues of Interest to the OEWG, By Theme", December 2019.

19 The academic debate on whether human rights are relevant in cyberspace is similarly polarized. Cfr. Graham, Mark. "There are No Rights 'in' Cyberspace", in *Research Handbook on Human Rights and Digital Technology,* pp. 24-32. Edward Elgar Publishing, 2019; Cristiano, Fabio. "Internet Access as Human Right: A Dystopian Critique from the Occupied Palestinian Territory", in *Human Rights as Battlefields,* pp. 249-268. Palgrave Macmillan, 2019.

20 The United Kingdom insists that 'discussion regarding the consequences and the impact of cyber operations such as the loss of life, and negative impact on economies, development, and human rights could be emphasized here'. Similarly, France argued that 'the information in paragraph 10, which aims to highlight how information technology issues are interconnected and influence other areas of the work of the United Nations - peace and security, human rights and sustainable development-could come earlier in the text'. The United States welcomes the strong relevance given by the document to the application of international human rights law to state-sponsored cyber operations. This element is further stressed by France: 'international human rights law is only considered through a simple mention of its applicability, whereas the issues of protection of personal data and the use of cyber space as a place to exercise fundamental freedom are today essential.'

21 As argued by Russia in their response to the OEWG's pre-draft 'considerable number of questions, which are not directly related to the problem of ensuring international peace and security (issues of the UN First Committee) are unreasonably included in the 'pre-draft' of the report'. In particular, the Russian response further stresses that 'redundant references to the problems of sustainable development, including its social aspects, human rights and gender equality, which, as mentioned in the text, fall within the competence of other UN bodies look, especially inappropriate'. Along the same line, China's response argues that sustainable development, gender and equality, and human rights are 'anything but a priority' for cyber security. In lieu of these, the Chinese statement suggests that a number of other issues should be prioritized by the OEWG: 'issues such as cyber sovereignty, supply chain security, protection of critical infrastructure, refraining from unilateral sanction and fight against cyber terrorism.'

22 Cfr. Broeders, Dennis, Liisi Adamson, and Rogier Creemers. *Coalition of the Unwilling? Chinese and Russian Perspectives on Cyberspace*. The Hague Program for Cyber Norms Policy Brief. November 2019.

23 Human Rights Watch. "China: Disclose Details of Terrorism Convictions", New York, 16 March 2017.

security.[24] As argued in Chapter 5 by Claessen, Russian authorities leverage counter terrorism discourse to impose strict restrictions with regards to content moderation as well as to control (or ban) tech companies and social media platforms.

As national strategies for countering terrorism in cyberspace increasingly relate to online content, actors other than the state – social media platforms, tech companies, surveillance technologies, automated machines, algorithms, etc. – become responsible for national security.[25] On this terrain, Mignot-Mahdavi (Chapter 6) shows how France has taken a leading role in fostering international cooperation on terrorist contents moderation by partnering with tech companies, in ways that have raised concerns – both nationally and internationally – in relation to freedom of expression. Along the same lines, the EU has promoted comprehensive regulations on terrorist contents moderation, receiving similar critiques with regards to human rights – as described by Wittendorp in Chapter 7.

In sum, the different essays in this collection point at a lack of clarity in the language used in the national context of cyber terrorism and 'terrorist use' of the internet more in general. In fact, these two tend – in different degrees – to increasingly merge and justify the application of pre-emption strategies to low-impact cyber activities and even to online content moderation. In this sense, the international diplomatic language needs to be careful in framing the possible threat of cyber terrorism in vague terms. As shown throughout this edited collection, the analyzed national legislations blur – to different extents – the boundaries between destructive cyber terrorism and other terrorist activities in cyberspace, thus extending counter terrorism responses designed for the former to the latter.

Besides the risk of weakening the UN's broader position as normative advocate of human rights, an unclear diplomatic language on cyber terrorism also risks to provide legitimacy to those countries that are keen to stretch the terrorist 'label' to domestic oppositions or minorities. Concluding, the framing of unwanted cyber activities in discourses on terrorism can allow these regimes to recur to a wider set of repressive policies and to deflect international criticism by aligning themselves to similar international discourses. In the long run, this might prove to be *kryptonite* for human rights in general and also for the United Nations' ambition of mainstreaming their protection into international cyber security.

24 Human Rights Watch. "Russia: Growing Internet Isolation, Control, Censorship", New York, 18 June 2020.

25 The criminologist David Garland has defined this process of delegation as 'responsibilization'; cfr. Garland, David. *The culture of control: Crime and social order in contemporary society.* University of Chicago Press, 2012. On the same debate, see also Douek, Evelyn. "The Rise of Content Cartels", Knight First Amendment Institute at Columbia, 11 February 2020.

2. United States and cyber terrorism: from ideological cradle to the test of international standards

Krisztina Huszti-Orban

For the past two decades, security sector actors have been consistently warning about the potentially crippling but elusive threat of cyber terrorism.[26] As such, cyber terrorism figures prominently on many domestic threat assessment lists, therein comprised the United States of America.[27] While there seems to be little controversy among policy-makers and other government stakeholders about the pertinent place the prevention and deterrence of cyber terrorism occupies among defense priorities, there seems to be less unambiguous guidance as to the scope of the phenomenon covered by the term "cyber terrorism." Whereas definitional lacunae may at times be dismissed due to a "we-know-it-when-we-see-it" attitude, it is doubtful that many jurisdictions (including the US) can claim to have developed a unitary, internally consistent conceptualization of the notion. This brief will focus on the ways in which cyber terrorism is approached in the United States counter-terrorism-related legal and policy framework while assessing whether and, if so, how, related definitions have been influenced by and are conform with relevant international standards. Whereas a comprehensive analysis of the US legal and policy framework falls outside of the its purview, the brief hopes to provide a sensible overview of select pertinent issues.

International standards serving as benchmark for the analysis

Despite the multitude of international instruments addressing issues related to the prevention and countering of terrorism,[28] there is no internationally accepted binding definition of what terrorism entails.[29] This gap should however not be used to underplay the broad agreement on several main

26 See, for example, National Research Council, *Computers at Risk: Safe Computing in the Information Age.* National Academy Press, Washington, DC, 1991; Keith Lourdeau, Deputy Assistant Director, Cyber Division, FBI, "Testimony before the Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security", 24 February 2004; Jarvis, Lee, Lella Nouri, and Andrew Whiting. "Understanding, Locating and Constructing Cyberterrorism", in *Cyberterrorism,* pp. 25-41. Springer, New York, NY, 2014.

27 See, for example, Daniel R. Coats. "Worldwide Threat Assessment of the US Intelligence Community. Statement for the Record", Office of the Director of National Intelligence, 29 January 2019; McCarthy, Justin. "Americans Cite Cyberterrorism Among Top Three Threats to US", *Gallup News,* 10 February 2016; Cronin, Cat. "The Growing Threat of Cyberterrorism Facing the US", *American Security Project,* 25 June 2019.

28 See United Nations Office of Counter-Terrorism. "International Legal Instruments".

29 The draft comprehensive convention on international terrorism has been under negotiation at the United Nations General Assembly since 1996. For example, see Hmoud, Mahmoud. "Negotiating the Draft Comprehensive Convention on International Terrorism: Major Bones of Contention", *Journal of International Criminal Justice* 4/5, (2006): 1031–1043. Definitions found in other binding instruments reflect the scope of the relevant instrument and are, as such, limited in ambit. Other, non-binding, definitions of terrorism include the definition developed by the mandate of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism. In the view of the mandate, the definition reflects best practice in countering terrorism, pursuant to an analysis undertaken on the basis of consultations and various forms of interaction with multiple stakeholders, including governments. See A/HRC/16/51, Practice 7.

constitutive elements of the offense of terrorism.[30] For the purposes of this analysis, the paper will use the delineation of terrorism advanced by the Security Council in its resolution 1566 as reference point.[31] While this definition is not specific to cyber terrorism, cyber terrorism would reasonably need to reflect the main elements of the offense of terrorism, so as to allow for a proper delineation between cyber terrorism and other related legal categories, such as cybercrime. The Security Council defined terrorism as encompassing:

> [C]riminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act, which constitute offences within the scope of and as defined in the international conventions and protocols relating to terrorism [...].[32]

Definitions of cyber terrorism

There is no statutory definition of cyber terrorism in US federal law. However, several policy definitions have been advanced in past decades. Mark Pollitt, of the Federal Bureau of Investigations (FBI), described cyber terrorism as "[t]he premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub-national groups or clandestine agents."[33] Keith Lourdeau, as Deputy Assistant Director of the FBI's Cyber Division advanced a somewhat modified definition during a hearing before the Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security, stating that cyber terrorism was "[a] criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services, where the intended purpose is to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social or ideological agenda."[34]

The two definitions quoted above have some commonalities (such as references to such cyberattacks resulting in real-life harm as well as a focus on the motivation of the conduct) but also significant differences in their scope and the constitutive elements they focus on. The understanding of cyber terrorism advanced by Pollitt is the narrower and more confined of the two.[35] It also seems to be more widely referenced by relevant stakeholders. The definition shared by Keith Lourdeau sets out the proposed elements of cyber terrorism in more detail. While it does not explicitly refer to any international standards, it reflects, to a degree, some of the components contained in Security Council

30 See A/73/361, para. 9. The key contentions in relation to the draft comprehensive convention include the question as to whether States can be perpetrators of terrorism as well as controversy over the circumstances under which the conduct of national liberation movements can be considered terrorism. The present brief will not tackle questions related to any of these considerations.

31 While one can find broader constructions of the notion of cyber terrorism, used in diverse contexts, including in academia, as well as public or journalistic discourse, it is important to assess relevant conceptualizations by public authorities against an authoritative definition.

32 S/RES/1566 (2004), para. 3.

33 Pollitt, Mark M. "Cyberterrorism—fact or fancy?", *Computer Fraud & Security* 2, (1998): 8-10. See also, Everard, Paul. "NATO and Cyber Terrorism", in *Responses to Cyber Terrorism,* NATO Science and Peace Security Series, (2008): 119.

34 See Lourdeau, 2004. The same definition has also been referenced as a definition adopted by the National Infrastructure Protection Center. See Everard, 2008.

35 Note that Pollitt's definition does not include the requirement that relevant conduct be perpetrated with a special intent aimed at causing terror or unlawfully compel governments to action.

resolution 1566. At the same time, it is also considerably more expansive than the understanding advanced by the Security Council. In particular, it encompasses criminal acts resulting in "violence" and in the "destruction and/or disruption of services." This covers a broader range of conduct than acts that "cause death or serious bodily injury" or consist in the taking of hostages.

Furthermore, while the UN restricts the scope to conduct aimed to "provoke a state of terror," "intimidate a population" or "compel" government to act in a certain way, this latter FBI definition is considerably looser by only requiring that such conduct "create fear by causing confusion and uncertainty within a given population," with the goal of "influencing" a government or population to accept the perpetrator's "political, social or ideological agenda."[36] As such, the way in which cyber terrorism is construed in accordance with this definition allows for it to potentially encompass an expanded category of conduct, including conduct that is not genuinely terrorist in nature. Human rights mechanisms, most notably the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, have consistently highlighted the importance of ensuring that relevant definitions adopted and implemented by States are narrowly construed and restricted to offences that "correspond to the characteristics of conduct to be suppressed in the fight against international terrorism, as identified by the Security Council."[37]

Possible approaches to delineating the "cyber element"

Starting from the premise that the notion of cyber terrorism ought to mirror the elements of the crime of terrorism as defined for "offline" purposes, having a common understanding of the types of uses of computer and Internet communication technology (ICT) encompassed within the "cyber" element of cyber terrorism facilitates the delineation between (1) cybercrime and cyber terrorism; and (2) cyber terrorism and terrorism-related incidental offences where at least part of the conduct was carried out through a cyber medium.[38]

Noticeably, overbroad definitions of terrorism and actor-focused qualifications[39] may lead to the blurring of the line between cyber terrorism and different types of cybercrime. Under such approaches all or most (criminal) conduct perpetrated by a terrorist group[40] is equated to terrorism by virtue of having been committed by a terrorist actor. These approaches, while increasingly common, may lead to outcomes that are at odds with international standards relevant to countering terrorism, including international human rights law. Moreover, if the conceptualization of cyber terrorism encompasses all criminal activity provided any part of the conduct, including preparatory acts, was carried out through an online medium, even if this "cyber element" was incidental or negligible,[41] such approach would lead to a considerable broadening of conduct that could be

36 In one sense, however, both definitions are narrower than the definition of the Security Council. While terrorist acts are frequently committed with political, ideological or other motives, UN Security Council resolution 1566 (2004) does not require that such motives underpin terrorist acts.

37 In this sense, see A/HRC/16/51, paras. 26-27.

38 Proper distinction between cyber terrorism and cyber armed conflict is similarly crucial. Discussing the challenges of such delineation is however beyond the scope of the current brief.

39 Actor-focused qualification refers to regulatory approaches that fixate on the proscribed status of actors (such as terrorist groups) in determining the category the criminal conduct attributable to such actors falls into.

40 This would include, for example, sexual or gender-based violence, hacking, etc.

41 See, for example, McGuire, Michael R. "Putting the 'cyber' into cyberterrorism: re-reading technological risk in a hyperconnected world", in *Cyberterrorism,* pp. 63-83. Springer, New York, NY, 2014.

qualified as cyber terrorism and thus come within the scope of relevant domestic laws and policies. The impact of such sweeping approaches is considerable having in mind that terrorism-related offences increasingly have an online component.[42] Expanding the reach of cyber terrorism regulation beyond offences the commission of which makes use of and is dependent upon ICTs "both as a concept, and for its execution"[43] risks overextending the category of cyber terrorism. At the same time, US law arguably provides insufficiently precise guidance on "the role technology plays in defining cyber terrorism as an offence."[44]

Investigating and prosecuting cyber terrorism and cyber terrorism-adjacent conduct

The term "cyber terrorism" is introduced in Section 814 of the USA Patriot Act[45] focusing on "deterrence and prevention of cyber terrorism." It may be inferred that the definition of "acts of terrorism transcending national boundaries" found in 18 US Code Section 2332b is relevant to this context as well. Section 814 amends Section 1030, Title 18 of the US Code to broaden the scope of its provisions, increase related penalties and clarify the categories of protected computers. These statutory provisions appear to be to be the main applicable working legal construct when it comes to cyber terrorism investigation and prosecution.[46] It is important to note that the stated purpose of Section 814 is prevention and deterrence. For this reason, relevant acts falling with Section 1030 of the USS are not technically qualified as (cyber)terrorism but, rather, their pursuit under criminal law is considered a prevention and deterrence tool in the context of the cyber terrorism threat. At the same time, the scope of these statutory provisions (referring to cybercrime and associated outcomes such as illicit access to computers) may not cover the full scope of conduct encompassed by the policy definitions advanced by the FBI addressed *supra*.

This background is also reflected in cyber terrorism-related prosecutions. Perhaps the most prominent case would be that of Ardit Ferizi, convicted of providing material support to a terrorist organization through accessing a protected computer without authorization and unlawfully obtaining information,[47] conduct described by then-Assistant Attorney General for National Security, John Carlin as a "*combination of terrorism and hacking*."[48]

42 For example, most financial transactions through the formal financial system involve the use of ICTs. This is also true for transactions involving cryptocurrencies, even when these eschew the formal banking system. As a result, terrorist financing increasingly has an online component. Similarly, terrorist actors use cyberspace for planning, propaganda and recruitment purposes. Consequently, related offences are frequently perpetrated online, at least in part. See, for example, United Nations Office on Drugs and Crime. *The use of the Internet for terrorist purposes*. United Nations, New York, 2012.

43 See, for example, McGuire, 2014, p. 67.

44 *Ibid.,* p. 69.

45 United States Congress. "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" (US Patriot Act), 26 October 2001. Among others, Sections 202, 212 and 217 of the Patriot Act may also be employed to address cyber terrorism-related threats. However, these provisions have reportedly not or infrequently been used to investigate and prosecute cyber terrorism. See Soesanto, Stefan. "Cyber Terrorism. Why it exists, why it doesn't, and why it will", Elcano Royal Institute, 17 April 2020.

46 Theohary, Catherine A. and John W. Rollins. "Cyberwarfare and Cyberterrorism: In Brief", Congressional Research Service, Washington DC, 27 March 2015.

47 Department of Justice Office of Public Affairs. "ISIL-Linked Kosovo Hacker Sentenced to 20 Years in Prison", Office of Public Affairs, 23 September 2016.

48 *Ibid.*

Conclusion

As of now, the United States has not been successfully targeted by a sophisticated act of cyber terrorism. However, experts deem that the risk of such attacks occurring will continue to rise, becoming ever more concrete and realistic in the relatively near future. At this point in time, the US has no statutory definition of cyber terrorism, but security sector actors have developed and employ a number of policy definitions in this respect. Should relevant acts be perpetrated, the statutory framework provides for several possibilities to investigate and prosecute such conduct, however, not as cyber terrorism but as terrorism-related offences and different manifestations of cybercrime. Having reflected on the reasons for the lack of a statutory definition of cyber terrorism in the US, experts seem to consider that this lacuna is due to the difficulty in identifying the perimeters of the phenomenon, including the type and scope of cybertechnology use required for classifying conduct as cyber terrorism. Moreover, in an area of fluidity and unpredictability, "retaining strategic maneuverability" in this respect may be seen as a definite advantage by policy-makers.[49]

49 See Soesanto, 2020.

3. United Kingdom: the constructed threat of cyber terrorism

Gareth Mott

Although it has existed since the 1980s in a science fiction capacity,[50] the term 'cyber terrorism' has not been conclusively defined either within academia or indeed amongst policymakers internationally.[51] There has been sustained debate as to what this term may mean and indeed whether we should refer to the term cyber terrorism at all. Nonetheless, cyber terrorism has been 'spoken into existence';[52] it is a social construction of a threatening phenomenon, irrespective of legitimate claims that cyber terrorism has not yet occurred anywhere in the world.[53] This paper draws from – and builds upon – research and findings produced in the author's monograph, entitled *Constructing the Cyberterrorist: Critical Reflections on the UK Case,*[54] in order to articulate the manner in which British political discourse and legislation has 'securitized' the threat of cyber terrorism. To securitize an issue is to discursively elevate it from a 'political' realm, instead transposing it into an exceptional 'security' realm in which extraordinary policies may be implemented or reinforced.[55]

The UK is an interesting case study in relation to the construction of the threat of cyber terrorism, because the legislation under which incidences of cyber terrorism may be prosecuted pre-exists the discursive construction of the threat. Accordingly, such an activity would be prosecutable under the Terrorism Act 2000 in most instances, which, under Section (2)(e) of its definitions of terrorism includes attacks that are "designed seriously to interfere with or seriously disrupt an electronic system".[56] An attack that may not fit the parameters of the Terrorism Act - for instance, a serious or sustained attack perpetrated by a group not already included in the proscribed terrorist group list – could also be prosecutable under the Computer Misuse Act 1990.[57] However, it is important

50 Collin, Barry C. "The future of cyberterrorism: Where the physical and virtual worlds converge", *Crime and Justice International* 13/2, (1997): 15-18; Ballard, James David, Joseph G. Hornik, and Douglas McKenzie. "Technological facilitation of terrorism: Definitional, legal, and policy issues", *American Behavioral Scientist* 45/6, (2002): 989-1016.

51 Jarvis, Lee and Stuart Macdonald. "What is cyberterrorism? Findings from a survey of researchers", *Terrorism and Political Violence* 27/4, (2015): 657-678; Macdonald, Stuart, Lee Jarvis, and Simon M. Lavis. "Cyberterrorism Today? Findings From a Follow-on Survey of Researchers", *Studies in Conflict & Terrorism,* (2019): 1-26.

52 Conway, Maura. "Determining the role of the internet in violent extremism and terrorism: Six suggestions for progressing research", *Studies in Conflict & Terrorism* 40/1, (2017): 77-98.

53 Kenney, Michael. "Cyber-terrorism in a post-stuxnet world", *Orbis* 59/1, (2015): 111-128.

54 Mott, Gareth. *Constructing the Cyberterrorist: Critical Reflections on the UK Case*, Routledge, London, 2019.

55 Buzan, Barry, Ole Wæver, and Jaap De Wilde. *Security: A new framework for analysis*, Lynne Rienner Publishers, 1998.

56 UK Public General Acts. *The Terrorism Act 2000*, (Chapter 11); Walker, Clive. "Cyber-terrorism: legal principle and law in the United Kingdom", *Penn St. L. Rev.* 110, (2006): 625-665.

57 UK Public General Acts. *The Computer Misuse Act 1990*, (Chapter 18). The current maximum penalty under the CMA is ten years imprisonment and an unlimited fine. Breach of the Terrorism Act can receive a penalty of life imprisonment. Feasibly, in the context of the CMA, broader legislation can be applied, including the *Homicide Act 1957* and *Criminal Damage Act 1971*, where harmful intent beyond the act of hacking can be evidenced.

to stress that in British political discourse prior to 2010, the specific term 'cyber terrorism' was rarely, if ever, used. This status quo was perhaps indicative of the perception that whilst cyber terrorism was a distinct possibility, it was deemed improbable. In contrast, the perceived threat from nation-states – in particular China and Russia – was greater and therefore captured discussions around the protection of key British interests in cyberspace. In this vein, it was not surprising to find an excerpt from the 2009-2010 *Annual Report of the Intelligence and Security Committee,* which summarized part of a discussion with GCHQ representatives who, when questioned about the potential risk of cyber terrorism, dampened the threat on a relative basis.[58]

This discursive political scene changed substantively in 2010. As has become standard protocol in the UK, the then-new British Coalition government published a new *National Security Strategy* and *Strategic Defence and Security Review.* By overtly listing the key threats facing the UK and ranking these according to their likelihood and their propensity for harm, these documents sought to be the public face of UK security priorities for the duration of the Coalition government. Collectively, these documents established – on a formal basis – the stature of cyber terrorism as a Tier One threat to the UK. 'Tier One' is a classification that the British government used to distinguish the threats to national security that – taking account of both likelihood and impact – were the highest priority. This *Strategy* specifically cited cyber terrorism as a serious threat to the UK. It detailed "cyber-attack, including by other states, and by organized crime and terrorists" alongside 'international terrorism', 'international military crises', and 'major accidents or natural disasters' as a Tier One threat to British national security.[59]

This particular construction of the cyber terrorist threat was reiterated in the UK's first *Cyber Security Strategy,* which overtly raised the fear that the risk of terrorist application of significant cyber weapons was escalating.[60] This document also expressly distinguished between the general terrorist usage of online services (which it acknowledged were widespread) and the specific act of cyber terrorism itself (which it acknowledged had not yet occurred). The constructed securitization of the threat of cyber terrorism in the UK was reaffirmed by the updated 2015 version of the *National*

58 Intelligence and Security Committee. *Intelligence and security committee annual report 2009-2010*, London: Stationary Office. The report stated that: "GCHQ informed the committee that it is not known whether terrorist groups intend, or have the capacity, to launch significant attacks over the internet but this, along with extremist use of the internet, remains an area of considerable concern. Nevertheless, we have been told by GCHQ the greatest threat of electronic attack to the UK comes from state actors, with Russia and China continued to pose the greatest threat" (p. 20).

59 Cabinet Office. *A strong Britain in an age of uncertainty: the national security strategy*, Cabinet Office, London, 2010a; Cabinet Office. *Securing Britain in an age of uncertainty: the strategic defence and security review*, Cabinet Office, London, 2010b. The *Strategy* warned that: "attacks in cyberspace can have a potentially devastating real-world effect. Government, military, industrial and economic targets, including critical services, could feasibly be disrupted by a capable adversary. 'Stuxnet' ... was seemingly designed to target industrial control equipment. Although no damage to the UK has been done as a result, it is an example of the realities of the danger of our interconnected world). The *Review* highlighted that "the risks emanating from cyberspace (including the internet, wider telecommunications and computer systems) of one of the four Tier One risks to national security. These risks include... the actions of cyber terrorists ... these threats... are likely to increase significantly over the next five to ten years as our dependence on cyberspace deepens".

60 Cabinet Office. *The UK cyber security strategy: protecting and promoting the UK in a digital world*, Cabinet Office, London, 2011. The Cyber Security Strategy noted that: "cyberspace is already used by terrorists to spread propaganda, radicalise potential supporters, raise funds, communicate and plan. While terrorists can be expected to continue to favour high-profile attacks, the threat that they might also use cyberspace to facilitate or to mount a can attacks against the UK is growing. We judge that it will continue to do so, especially if terrorists believe that our national infrastructure may be vulnerable".

Security Strategy and the 2016 version of the *Cyber Security Strategy*.[61] It is therefore of note that these public facing security documents served two functions with respect to the debates around the threat of cyber terrorism in the UK. Firstly, the documents served to legitimize the discussion of cyber terrorism; this now became a bona fide part of discussions around British security in the contemporary networked era. Secondly, the documents also served to define the parameters of the debate by imposing a particular interpretation of what cyber terrorism is, and by process of elimination, what it is also therefore *not*. To be specific, the British construction of the threat of cyber terrorism is concerned with the potential use of cyber weapons by terrorist entities against critical national infrastructure. This is cogently distinguished from broader uses of online services by terrorist organizations.

With the parameters of the securitization of cyber terrorism in place, between May 2010 and June 2016 – the tenure of the Cameron Coalition and Conservative governments – discourse at the political level in the UK proliferated with the term 'cyber terrorism' and derivates thereof.[62] Several key findings can be raised. Notably, in over 100 distinct instances in which the threat of cyber terrorism was raised by Ministers, MPs and peers both inside and outside of the Chambers, there was no dissent. No political figure disputed the perception that cyber terrorism was an increasing threat. In some instances, the specter of cyber terrorism was cast in dire terms. Delivering a public-facing speech to GCHQ in November 2015, then-Chancellor George Osborne stated that:

> "the stakes could hardly be higher – if our electricity supply, or our air traffic control, or our hospitals were successfully attacked online, the impact could be measured not just in terms of economic damage but of lives lost … [so] when we talk about tackling ISIL, that means tackling their cyber threat as well as the threat of their guns, bombs and knives … the pace of innovation of cyber attack is breathtakingly fast".[63]

Broadly, there was a consensus view that cyber terrorism referred to hypothetical instances in which terrorist organizations attack critical infrastructure with cyber weapons; indeed, overt references to the *Strategy* and *Review* documents were widespread. Delivering a *Cyber Crime* speech in March 2013, James Brokenshire, then a Parliamentary Under-Secretary for the Home Office noted that:

---

61 Cabinet Office. *National security strategy and strategic defence and security review 2015: a secure and prosperous United Kingdom*, Cabinet Office, London, 2015; Cabinet Office. *National cyber security strategy 2016-2021*, Cabinet Office, London, 2016. The 2015 version of the *National Security Strategy* re-affirmed that: "the range of cyber actors threatening the UK has grown. The threat is increasingly asymmetric and global … nonstate actors, including terrorists and cyber criminals can use easily available cyber tools and technology for destructive purposes", and that these threats were 'significant and varied', including: "cyber terrorism … and disruption of critical national infrastructure as it becomes more networked and dependent on technology data held overseas". The *2016 Cyber Security Strategy* provided a measured assessment of the escalating threat: "terrorist groups continue to aspire to conduct damaging cyber activity against the UK and its interests. The current technical capability of terrorists is judged to be low … the current assessment is that physical, rather than cyber, terrorist attacks will remain the priority for terrorist groups for the immediate future … the potential for a number of skilled extremist lone actors to emerge will also increase, as will the risk that a terrorist organisation will seek to enlist an established insider. Terrorists will likely use any cyber capability to achieve the maximum effect possible. Thus, even a moderate increase in terrorist capability may constitute a significant threat to the UK and its interests".

62 After June 2016 there has been a marked decline in the use of the term 'cyber terrorism' and derivatives thereof; although this may be indicative of a relative dearth of parliamentary time available to consider this and other issues within proposed legislation and standing orders. Since June 2016 there have been five instances in which the threat of cyber terrorism has been raised in either Chamber. These instances adhered to the same structure of the discourse that preceded them.

63 Osborne, George. "Chancellor's speech to GCHQ on cyber security", Government Communications Headquarters, London, 17 November 2015.

> "to date, terrorists have not seen cyber attack as an important means of conducting their actions, although of course they use the internet to radicalise, spread propaganda, disseminate violent extremist material and communicate with each other. But we and other governments must be very mindful of the fact that this could change".[64]

In a similar vein, Baroness Neville-Jones, speaking during a *Tackling Online Jihad* conference as the Security Minister, informed her audience that there was a discernible risk:

> "likely to grow over time and which we monitor closely, that terrorists will develop serious cyber attack capabilities: by this I mean the ability to commit acts of terror by hacking into critical infrastructure and online systems. In some form, a cyber attack attempted by terrorists, if not inevitable, is of so great a likelihood that we bear it in mind in developing operational capabilities".[65]

Given that the threat of cyber terrorism targets technology, and is enabled by technology, one might expect to see references to the technology itself in the exhibited discourse of the threat. Significantly however, the political discourse was overwhelmingly interested in the *identity construct* of purported cyber terrorist actors, rather than the weapon systems themselves. The weapon systems were instead left in a neutral discursive space; the weapons themselves were neither good nor bad, and this evaluation revolved on the identity of the person or group deploying them.[66]

This author proposes that the constructed (and legislated) threat of cyber terrorism may have some indirect implications for digital rights and/or civil liberties, specifically with regard to the narrowing of the available political debate. Whilst the UK government has intermittently exhibited discourse relating to restricting access to, or use of, widespread encryption technologies, in an effort to restrict their untrammeled use by extremist organizations and other criminals, this discourse has largely not amounted to significant change in policy making terms.[67] With respect to the 'non-cyber terrorism' parameters of the Terrorism Act 2000, there are documented instances in which this legislation has been used in an aggressive fashion that arguably disproportionately undermined the civil liberties of individuals, particularly with respect to the application of Schedule 7.[68] Polling of the British populace has typically exhibited distinct – and persistent – sentiment on these issues. This polling has indicated that the British public value 'security' over 'privacy' with respect to online matters, and, even in the wake of the 2013 Edward Snowden revelations (which were described by then-MI5 chief Andrew Parker as a 'gift' for terrorists), the public held the view that intelligence agencies should have *greater* access to surveillance powers.[69] This public sentiment provided a backdrop of support for the Investigatory Powers Act 2016, which consolidated and legitimized existing large-scale surveillance practices.

---

64 Brokenshire, James. "James Brokenshire speech on cyber crime", Home Office, London, 14 March 2013.

65 Neville-Jones, Pauline. "Tackling online Jihad: Pauline Neville-Jones's speech", Home Office, London, 31 January 2011.

66 Cfr. Mott, 2019.

67 Travis, Alan. "Call for encryption ban pits Rudd against industry and colleagues", *The Guardian,* 26 March 2017.

68 Bowcott, Owen. "Terrorism Act incompatible with human rights, court rules in David Miranda case", *The Guardian,* 19 January 2016. Schedule 7 enables the police to stop, examine and detain passengers at transportation hubs. Individuals may be detained for up to six hours, and reasonable suspicion is *not* necessary.

69 Dahlgreen, Will. "Little appetite for scaling back surveillance", *YouGov,* 13 October 2013; Dahlgreen, Will "Broad support for increased surveillance powers", *YouGov,* 18 January 2015; Faulconbridge, Guy. "MI5 chief warns Snowden data is a 'gift' for terrorists", *Reuters,* 8 October 2013; Jordan, William. "Snowden revelations 'good for society'", *YouGov,* 18 April 2014.

However, with respect to the use of the legislation against instances of 'terroristic' electronic interference, there are few cases to speak of[70] and it would be difficult to categorically argue that the particular British construction of the threat of cyber terrorism has served to restrict digital rights or civil liberties. In contrast, as the annual UK's *Cyber Security Breaches Survey* routinely highlights, broader profit-driven hacking directly or indirectly impacting UK organizations is prolific, to the extent that many attacks are not reported and not investigated.[71] There is, of course, widespread political-level discourse in the UK concerning the threat of generic profit-driven cybercrime. It is notable, however, that the 'cyber terrorism' discourse in the UK appears to have operated on a standalone basis, separate to 'cybercrime' or indeed 'terrorism' more broadly construed. This author suggests that the construction of the threat of cyber terrorism in the UK is pre-emptive in the sense that it articulates the real possibility of terrorist usage of cyber weapons against critical national infrastructure. The discourse is also self-reflective (although not self-critical), in that it insulates itself against exhibiting limited shelf life by exclaiming that the threat of cyber terrorism is increasing over time. The constructed threat is therefore reflective of the Rumsfeldian[72] logic: the absence of evidence is not the evidence of absence.

This is not to say that the constructed threat does not have significant implications for freedom of debate and dissemination of knowledge in the UK. It is of note that the UK political discourse left the cyber weaponry itself in a neutral space; focusing instead on the 'bad' actors who may or may not deploy them. This has important ramifications in terms of legitimizing particular practices and also in silencing debates that might otherwise be warranted. The UK was one of the first countries in the world to recognize that it rigorously develops a cyber offensive arsenal,[73] but we have not had a public facing debate about the rationale and proportionality of these weapon systems. Cyber weapons are unlike any other weapon system. They do not weigh anything, they can be disseminated at the speed of light, they can be replicated with very little cost. They can also leak, to potentially devastating effect.[74] By 'securitizing' the threat of cyber terrorism, the UK political discourse arguably serves to legitimize UK state-oriented cyber weapon practices, whilst at the same time avoiding public-facing scrutiny of, and debate around, the weapon systems themselves. As British society becomes increasingly networked, with IT systems penetrating deeper into both the national economy and our daily lives, we may reach a point at which the (tacit) avoidance of a rational and mature public forum around the implications of cyber weapons becomes untenable.

---

70 In May 2017, British media outlets reported the successful prosecution of a 'cyber terrorist', Samata Ullah. Ullah, an autistic man from Cardiff, was sentenced to an eight-year term for distributing sensitive materials in USB cufflinks and advising suspected terrorist figures in Kenya about online anonymity. *The Times* and the *Evening Standard* labelled him a 'new and dangerous breed of terrorist', a 'cyber terrorist'; *The Sun* labelled him a 'James Bond Jihadi'. However, Ullah did not conduct any known cyberattacks per se. See Simpson, John and Duncan Gardham. "ISIS hacker who hid terror files on cufflinks is jailed", *The Times,* 3 May 2017; Mitchell, Jonathan. "Jailed: cyberterrorist Samata Ullah who used James Bond-style cufflinks to hide ISIS propaganda", *Evening Standard,* 2 May 2017; Lake, Emma. "Cuff him: 'James Bond Jihadi' Samata Ullah who used cyber cufflinks to hide ISIS data and was branded new breed of terrorist is caged", *The Sun,* 2 May 2017.

71 Ipsos Mori. *Cyber Security Breaches Survey 2019*, Department for Digital, Culture, Media and Sport, London, 2019.

72 Rumsfeld, Donald. "Press conference by US Secretary of Defence, Donald Rumsfeld", NATO HQ, Brussels, 7 June 2002.

73 Blitz, James. "UK becomes first state to admit to offensive cyber attack capability", *Financial Times,* 29 September 2013.

74 In April 2017, 300mb of cyber exploits for legacy Windows operating systems that had been developed by the National Security Agency (NSA) were released by the 'Shadow Brokers', who had been drip-feeding a cache of exploits for the preceding eight months. 'Eternalblue', a worm, was part of this cache and would later be re-purposed for the 'Wannacry' ransomware attack that affected thousands of organizations in the summer of 2017. See Goodin, Dan. "NSA-leaking Shadow Brokers just dumped its most damaging release yet", *Arstechnica,* 14 April 2017; Graham, Chris. "NHS cyber attack: everything you need to know about 'biggest ransomware' offensive in history", *The Telegraph,* 13 May 2017.

4. China: the 'three evils' of cyberspace and human rights

Siodhbhra Parkin

Since 2014, the Chinese government has formulated and implemented a wide range of laws, policies, and other directives to comprehensively strengthen the national security regulatory framework as it applies to cyberspace, including acts of cyber terrorism. These resulted in serious consequences for human rights defenders, independent journalists, and civil society actors. Several major pieces of national-level legislation are particularly useful in understanding the intersection of cyberspace regulation and counterterrorism policies, specifically: The *National Security Law* (2015), the ninth amendment to the *Criminal Law* (2015), the *Counterterrorism Law* (2016), and the *Cybersecurity Law* (2017). An important policy document, the 2016 "National Cyberspace Security Strategy," also outlined the concerns among Chinese policymakers that the Internet was being used as a tool to "incite, plan, organize, and carry out" acts of terrorism, separatism, and extremism – the so-called "Three Evils."[75]

Across these legislations and policy documents, the Chinese government set forth a broad conceptualization of key concepts including terrorism, extremism, and cyber security. Rather than define – or even mention – the term cyber terrorism (网络恐怖主义) specifically, legislators chose to adopt definitions of "terrorism" (恐怖主义) and "terrorist activities" (恐怖活动) that do not distinguish between the online or offline nature of actions including planning, fundraising for, encouraging, or coordinating terrorist attacks;[76] the Internet is a tool used in committing a crime, not an independent constitutive element of one.[77] As experts at the United Nations as well as other scholars and commentators have pointed out, the lack of specificity regarding definitions of central terms and concepts presents significant challenges from a human rights perspective, even as it preserves maximal flexibility and discretion for government actors in terms of choosing when, and against whom, to implement these provisions.[78]

75 Cyberspace Administration of China. *National Cyberspace Security Strategy* (国家网络空间安全战略), 27 December 2017. English translation can be found here.

76 The term "terrorism" is defined in Article 3 of the *2016 Counterterrorism Law* as any action taken to "create social panic, endanger public safety, violate persons or property, or coerce national organs or international organizations," without further specifying special conditions for addressing cyber-terrorism specifically. The *2017 Cybersecurity Law* makes mention of terrorism as one of a number of prohibited online activities only once, in Article 12.

77 United Nations Office on Drugs and Crime. *The use of the internet for terrorist purposes*, United Nations, Vienna, 2012: 29.

78 See, *inter alia,* Fionnuala Ní Aoláin, Leigh Toomey, Luciano Hazan, et al., "Comments on the effect and application of the Counter-Terrorism Law of the People's Republic of China OL CHN 18/2019", Office of the United Nations High Commissioner for Human Rights, Geneva, 2019: pp. 10-11; Jacque deLisle, "Security First? Patterns and Lessons from China's Use of Law to Address National Security Threats", *Journal of National Security Law and Policy,* (2010): 410-411; and Cong, Wanshu. "China's 2015 Counterterrorism Law", *Journal of Comparative Law* 11/2, (2016): 381.

Thus, in the Chinese law and policy context, cyber terrorism is best understood to refer to a whole range of online activities deemed to fall under the wide variety of actions prohibited and regulated under umbrella legislation recently passed or amended at the national level including the *Criminal Law* (2015), *Counterterrorism Law* (2016) and *Cybersecurity Law* (2017). By advancing the dual goals of expanding securitization and centralized control, this legislative approach to cyber terrorism is a clear example of the overall style of governance that has come to characterize President Xi Jinping's administration. In President Xi's own words, on the occasion of launching the Central Leading Group for Cyberspace Affairs in February 2014, "There can be no national security without cyber security."[79] In practice, this "security-first" approach to cyberspace and counterterrorism has had devastating consequences for the basic human rights of millions of ordinary people. The clearest example of this is, of course, the ongoing and massive rights violations in evidence in the Xinjiang Uighur Autonomous Region ("Xinjiang"), where an estimated one million Uighurs and other Muslim minority groups have been extralegally detained in specially built camps as part of a so-called "de-extremification" campaign.[80] Meanwhile, the Chinese government continues to operate one of the largest and most technically sophisticated systems for online censorship and surveillance of its own citizens.[81]

Merging different cyber domains

In addition to promoting similar political objectives for securitization and centralized control, the Party-state's recent efforts to comprehensively regulate cyberspace and significantly enhance its counterterrorism initiatives are also mutually reinforcing. In particular, both categories of legislation place heavy emphasis on policing the creation and dissemination of information online. As provided in the *Counterterrorism Law* (2016), for example, any online activity that directly or indirectly supports broadly defined "terrorist activities" or "terrorist groups" – and of especial note, the transmission of "extremist" content or propaganda – is illegal and punishable by law. The *Cybersecurity Law* (2017) echoes this, in addition to introducing new requirements and mechanisms intended to ensure the Party-state's capacity to surveil and control *any* online actor, starting with real-name registration and identification requirements, and provide such general definitions of illegal behaviors so as to preserve the state's ability to intervene in a wide range of instances.

Indeed, starting in 2014, Chinese government bodies and administrative agencies issued a flurry of laws, regulations, and other directives to consolidate control over the various elements of the cyberspace ecosystem and the various actors within those spaces. The frenetic burst of policymaking resulted in new regulations impacting nearly every online stakeholder, including network operators, critical information infrastructure operators, domain name service providers and users, Internet news units and content management personnel, various social media providers and users, and more generally, "individuals and organizations using [the] network." By the end of 2017, the fundamental framework of China's Internet regulation was in place, stretching over a patchwork of laws and policies but united under an overarching and unambiguous ideological umbrella.

79 The Central People's Government of China. "The Central Leading Group for Cybersecurity and Informatization Holds its First Meeting" (中央网络安全和信息化领导小组第一次会议召开), 27 February 2014.

80 Nebehay, Stephanie. "U.N. says it has credible reports that China holds million Uighurs in secret camps", *Reuters,* 10 August 2018; Ramzy, Austin and Chris Buckley. "'Absolutely No Mercy': Leaked Files Expose How China Organized Mass Detentions of Muslims", *New York Times,* 16 November 2019.

81 Qiang, Xiao. "Liberation Technology: The Battle for the Chinese Internet", *Journal of Democracy* 22/2, (2011): 47-61.

Concerns about cyber terrorism and cybercrime more generally were fully embedded into this regulatory framework. Apart from the national-level legislation already discussed, some of the key policies included the following: "Ministry of Industry and Information Technology Notice on Cleaning Up and Regulating the Internet Access Services Market" (2017); "Internet Post and Comment Services Management Provisions" (2017); and the "Provisions on the Security Assessment of Internet Information Services that have Public Opinion Natures or Social Mobilization Capacity" (2018). Following passage of the *Counterterrorism Law* (2016), authorities in Xinjiang also passed two significant implementing regulations that contained specific provisions against sharing disseminate objectionable content over the Internet, which have been used to bolster the legal and policy justifications for the mass detention and surveillance of ethnic Uighurs and other Muslim minority groups: "Xinjiang Implementing Measures for the PRC Counterterrorism Law" (2018); and the "Decision to Revise the 'Xinjiang Uighur Autonomous Region Regulation on De-extremification'" (2018).

Finally, in May 2018, the Supreme People's Court, Supreme People's Procuratorate, Ministry of Public Security, and Ministry of Justice issued joint guidelines on legal procedures and penalties for crimes involving terrorism. This document, entitled "Opinions on Several Issues on the Application of Law in Cases of Terrorist Activities and Extremism Crimes," confirmed that individuals who write, publish, broadcast, or advocate content relating to terrorism or extremism either offline or online are, indeed, criminally liable.[82] In this way, legitimate concerns about the use of the Internet as a tool for recruiting, financing, or carrying out acts of terrorism have been used to legitimize an approach to policing online activities in practice that, in the absence of a functioning rule of law, is extremely problematic from a human rights perspective.

Chinese regulations and freedoms: from international standards to national debate

As a matter of straightforward statutory interpretation, the key elements of the *Counterterrorism Law* (2016) and other legislations are not inconsistent with international frameworks. Rather, most of the issues with regards to digital rights emerge in the course of implementation within a system exhibiting severe rule of law defects. United Nations counterterrorism experts have drawn attention to this issue on multiple occasions; most recently, in an open letter from several Special Rapporteurs and representatives of various working groups and treaty bodies, experts noted their concern that provisions in the *Counterterrorism Law* disallowing or shutting down Internet telecommunications services under an overly broad of terrorism may impact rights to freedom of expression, access to information, and privacy.[83] The censorship mechanisms and content controls established in the *Cybersecurity Law* (2017) also raised concerns from international stakeholders regarding these same core rights and freedoms.[84]

82 Ministry of Public Security of the People's Republic of China. "Opinions on Several Issues on the Application of Law in Cases of Terrorist Activities and Extremism Crimes from the Supreme People's Court, Supreme People's Procuratorate, Ministry of Public Security, and Ministry of Justice" (最高人民法院、最高人民检察院、公安部、司法部关于办理恐怖活动和极端主义犯罪案件适用法律若干问题的意见), 5 May 2018.

83 Ní Aoláin et al., 2019: 11.

84 Kaye, David. "Promotion and protection of the right to freedom of opinion and expression" (A/71/373), United Nations General Assembly, New York, 6 September 2016: 6.

At the same time, on the international stage, Chinese officials have sent clear signals about their intention to work with other states in developing counterterrorism strategies and frameworks for cyberspace. While the United Nations remains its primary forum for engaging the international community on counterterrorism initiatives, it has been increasing its efforts to approach other actors in multilateral, bilateral, or regional forums in recent years – including raising the subject of countering cyber terrorism specifically.[85] For example, at the 2019 UN Security Council Briefing on "Threats to International Peace and Security Caused by Terrorist Acts," Ambassador Wu Haitao stated that "we [the international community] should…stop terrorist organizations from misusing the Internet and telecommunications technologies. We should support Member States to fully implement the Madrid Guiding Principles and the Addendum thereto…We should focus on enhancing international cooperation in combating cyber terrorism, terrorist financing and the spread of extremist ideologies."[86]

Outside of policy documents, the term cyber terrorism is usually used in the context of references to international cooperation and exchanges. This includes documents like the State Council Information Office brief on counter-terrorism efforts in Xinjiang as well as formal reports on China's cyber terrorism exercises with partner nations in the Shanghai Cooperation Organization. Beyond this, there are extensive government-led initiatives to promote "positive energy and content" online and discourage sharing or dissemination of objectionable content. The formation of the Central Leading Group for Cyberspace Affairs in February 2014 heralded a new direction for consolidation of control over Chinese cyberspace. Headed by President Xi Jinping, the Leading Group was tasked to exercise centralized leadership and coordinate important cyber security and informatization efforts. The Cyberspace Administration of China was subsequently established as the enforcement arm of the Leading Group. In August 2014, the State Council authorized the CAC to manage Internet information and content across the country, including supervision and law enforcement. The CAC soon centralized the regulatory power of Chinese Internet and brought definite structure to the previously scattered Internet regulatory regime.

Apart from the CAC, the other two main regulatory bodies of Chinese cyberspace are the Ministry of Industry and Information Technologies ("MIIT") and the Ministry of Public Security. The MIIT focuses on the administration of Internet industry, telecommunication and Internet infrastructure building. Meanwhile, the MPS focuses on cyber security, crime prevention, and responding to cybercrime and illegality. The CAC, MIIT, and MPS are identified as the three main regulators for supervision and management of cyber security in the *Cybersecurity Law* (Article 8). The MPS is also directly involved in the implementation of the *Counterterrorism Law* (Article 8), and in cases where both national security and cyber security are implicated, there is extensive coordination across the relevant government departments.

85 Bureau of Counterterrorism. "Country Reports on Terrorism: 2017", United States Department of State Publication, September 2018.

86 Wu, Haitao. "Statement by Ambassador Wu Haitao at Security Council Briefing on Threats to International Peace and Security Caused by Terrorist Acts", United Nations Security Council, New York, 11 February 2019.

In terms of formal legal action in the area of cyber terrorism, what publicly available data exists suggests that most prosecutions that may be categorized in this way involve the creation, possession, or dissemination of materials determined by authorities to be "terrorist" or "extremist" in nature.[87] This finding is consistent with the considerable number of legislations and policies discussed elsewhere in this analysis that are expressly designed to extend control over the creation and sharing of information. At the same time, the well-documented tendency of the Chinese Party-state to keep information deemed "sensitive" a closely guarded secret makes it impossible for an objective analysis of the implementation of the *Counterterrorism Law, Cybersecurity Law,* and other legislations that touch on cyber terrorism to be made—itself an indication that there are few robust, evidence-based measures in place to ensure there is ample protection for marginalized and vulnerable groups.

There is no shortage of evidence demonstrating that the Party-state cyber security and counterterrorism apparatuses in China is being mobilized against civil society advocates, rights defenders, independent journalists, as well as ordinary citizens.[88] From massive, technically sophisticated surveillance campaigns to abuses of facial recognition technologies to systemic efforts to monitor and censor free expression online, Chinese cyberspace has been increasingly subject to the control of authorities. Meanwhile, it is currently estimated that between 1-3 million people remain in some form of detention or surveillance in what have been variously described as "camps" or "re-education centers" in the Xinjiang Uyghur Autonomous Region in order to undergo so-called "de-extremification" to prevent future terrorist attacks.[89] Unfortunately, the lack of meaningful checks on government authority means that absent intervention by the international community or domestic reform, such abuses are likely to continue grow in both size and scope. While efforts have been made at the level of the United Nations and others to document the myriad abuses of fundamental rights to access information and freedom of information originating from and evident in the recently established cyber security and counterterrorism legal frameworks, as of this writing, much more remains to be done.[90]

87 Bureau of Counterterrorism, 2018: 52.

88 See, *inter alia,* Freedom House. "Freedom in the World 2020 – China Report"; and Human Rights Watch, "World Report 2020: China's Global Threat to Human Rights".

89 Zenz, Adrien. "Brainwashing, Police Guards and Coercive Internment: Evidence from Chinese Government Documents about the Nature and Extent of Xinjiang's 'Vocational Training Internment Camps'", *Journal of Political Risk* 7/7, 2019.

90 Human Rights In China. "Regulatory Framework, Surveillance Industry In China", Submission to the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", 15 February 2019.

5. Russia: cyber terrorism as an issue of information security

Eva Claessen

Cyber terrorism in Russian policy

The Russian approach to countering cyber terrorism is not easily determined. Part of the reason for this is the fact that the term itself is not used in domestic policy- or legislative documents. This provides a puzzle for determining not only a Russian definition of the term, but also the main policy priorities in countering terrorist activities in the online information space. Additionally, the conceptualization of the term becomes more difficult due to the fact that it is approached from the perspective of information security which is much broader in scope than the concept of cyber security. The preference for this term implies a more holistic approach towards cyber security, which encompasses both threats of a technological nature, as well as threats concerning the dissemination of information and content.[91] This broad approach to protect national security in cyberspace implies the need to counter both technological threats and 'threats of content'.

Due to this difference in terminology, there is no cyber security strategy for the Russian Federation. Rather, threats in the online information space, including terrorist threats, are outlined in the 2016's Doctrine of Information Security. It needs to be noted that also in this document a term like "cyber terrorism" is not used to denote terrorist activities specific to the online information space. Furthermore, it is only in its most recent publication (2016) that the doctrine went beyond mere mentions of the potential threat of "activities of international terrorist organizations".[92] Additionally, while the previous iteration (2000) did provide ample reflection on the need to protect Russia's information infrastructure, the link at this time was not yet made with potential threats from terrorist or extremist organizations. This changed with the 2016 doctrine, which listed the following threats associated with terrorist activities in cyberspace in the section on the "basic information threats":

1. The use of "mechanisms of information influence [...] with the goal of inflaming interethnic and societal tension, as well as inciting ethnic and religious hate or enmity
2. The propagation of extremist ideology and the recruitment of new members
3. The active creation of "means of destructive influence on objects of critical information infrastructure for illegal purposes".[93]

91 Nocetti, Julien. "Contest and conquest: Russia and global internet governance", *International Affairs* 91/1, (2015): 111-130.

92 The Ministry of Foreign Affairs of the Russian Federation. *Doctrine of Information Security of the Russian Federation*, 5 December 2016.

93 *Ibid.,* Art. 3 (§13).

It is only recently that the potential threat towards critical (information) infrastructure is made explicit in relation to terrorist activities. The first two aforementioned threats were already grounded in the 2006 "Concept for the Counteraction of Terrorism in the Russian Federation",[94] in which the use of information technologies for terrorist purposes was mainly related to the "diffusion of the idea of terrorism and extremism through the Internet".[95] Since the nature of this threat was at this point in time largely content based the main measures proposed to counteract it were two-fold: (1) regulating the use of information and communication systems;[96] and (2) the protection of the Russian information space.[97] The recent incorporation of the potential terrorist threats to objects of critical information infrastructure seems to be connected to an ongoing shift in focus from the regulation of content alone towards increasingly explicit efforts to centralize control over information infrastructure. Illustrative of this is the mention of the need to protect Russia's critical information infrastructure in the 2015 Strategy for National Security,[98] the disruption of which is listed as one of the main aims of the activities of terrorist and extremist organizations.

While these priorities on countering terrorist activities in cyberspace are becoming more concrete, the lack of an official definition of what cyber terrorism is and what exactly constitutes a terrorist activity in cyberspace, complicates determining the main approach that is used to counter these activities. The fact that cyber terrorism is not directly mentioned in these documents suggests that the phenomenon has in the past not been approached as a separate category of terrorism, but rather as the transfer of terrorist activities from the physical realm to the virtual one. Following the definition of the 2006 law "on the counteraction of terrorism", this would include the propaganda of terrorist ideology, the planning and committing of a terrorist act, as well as recruitment. In this sense, it did not yet include potential terrorist attacks on critical (information) infrastructure.

However, this does not mean that there is no debate on the need for more legislation aimed specifically at countering this phenomenon. It is just, that up until the period of 2014, this debate was mainly geared towards the development of international legal instruments as well as deepening multilateral, bilateral and regional cooperation in this regard. This point was made for example by Foreign Minister Sergei Lavrov during a statement to the State Duma after the introduction of the 2006 law on countering terrorism.[99] In his statement, Sergei Lavrov highlighted the necessity for an international definition of terrorism through the creation of a "comprehensive convention on international terrorism", an exercise, which according to him had been slowed down due to the fact that "some states advocate the admissibility of essentially terrorist methods in the struggle for national liberation and against foreign occupation".[100] Because of this, he emphasized the potential "pioneering, breakthrough role" for regional organizations in this regard. Taking the Council of Europe

94 Russian Federation. "Federal Law N°35-F3 on the Counteraction of Terrorism", 6 March 2006.

95 *Ibid.,* Art. 2 (§11).

96 *Ibid.,* Art. 2 (§21).

97 *Ibid.,* Art. 2 (§15).

98 Russian Federation. *National Security Strategy*, 31 December 2015. An unofficial translation can be found here.

99 State Duma of the Russian Federation. "Transcript of the Fourth convocation of the State Duma of the Federal Assembly of the Russian Federation: On the strengthening of international cooperation in the area of insuring security and the counteraction of international terrorism", 7 June 2006.

100 *Ibid.*

Convention on the Prevention of Terrorism as an example, Lavrov proposed the creation of similar conventions with "regional organizations that are close to Russia in the geographical and political sense"[101] including the CIS, CSTO, and the SCO.[102]

In the context of creating international mechanisms aimed at countering cyber terrorism, Russia has consistently emphasized the need to respect states' sovereign right to construct its own legislative framework to counter issues concerning information security, as well as the principle of non-intervention. An example of this is Russia's 2017 draft for a UN "Convention on cooperation in combatting cybercrime"[103] to replace the 2001 Budapest Convention. In explaining the rationale behind this proposal, Andrey Krutskikh – the special representative for the Russian Federation at the UN on international cooperation in the field of information security – highlighted that the main reason for putting forward a new convention was to "modernize" the Budapest convention to include new types of cybercrime, in particular the issue of cyber terrorism.[104] An additional and possibly more crucial reason in this regard was the Russian criticism of article 32 paragraph B in the Budapest convention which provides the signatories with the right to "access or receive [...] stored computer data located in another Party".[105] This is perceived as providing other states with the possibility of threatening Russian national security and sovereignty. Therefore, the draft convention proposed by Russia was presented as a reflection of its efforts in promoting multilateral cooperation to address threats to information security. At the same time, it highlighted the sovereign right of states to govern their respective information space within the confines of domestic legislation.

From content controls to infrastructural controls: the impact on digital rights

Russia's domestic legislative framework aimed at ensuring information security has recently shown a similar turn towards emphasizing state sovereignty in the information space. More specifically the law on the sovereign Runet,[106] features several elements aimed at achieving greater government control over the Internet infrastructure. This includes the requirement for ISPs to install DPI equipment on their network to provide Roskomnadzor with the possibility of filtering traffic and limiting access to information resources that are forbidden in the Russian Federation. Additionally, a system is put in place to allow for Roskomnadzor to centralize the management of the routing of traffic through a list of pre-approved IXPs in case of threats to the network.[107] While this law was not specifically introduced in relation to cyber terrorism, but rather to protect Russia against potential Internet shutdowns initiated by foreign actors, the law does have a significant impact on the development of legislation on countering terrorist activities online.

101 *Ibid.*

102 Examples of bilateral accords in this context are: the "Shanghai convention on combatting terrorism, separatism and extremism", 2001; and the "Agreement between the government of the Russian Federation and the government of the Chinese People's Republic on cooperation in the area of insuring international information security", 30 April 2015.

103 United Nations General Assembly. "Letter of the Russian Federation to the Secretary General: Draft United Nations Convention on Cooperation in Combatting Cybercrime" (A/C.3/72/12), 16 October 2017.

104 Peters, Allison. "Russia and China Are Trying to Set the U.N.'s Rules on Cybercrime", *Foreign Policy,* 16 September 2019.

105 Council of Europe. "Budapest Convention on Cybercrime ETS No. 185", Treaty Office, Strasbourg, 23 November 2001.

106 Russian Federation. "Federal law No. 90-FZ on amendments to the Federal law "On communications" and the Federal law "On information, information technologies and information protection"", 1 May 2019. An unofficial translation can be found here.

107 *Ibid.*

This development is particularly important, because it features in a larger evolution of internet regulation moving away from mere content control towards infrastructure controls. A report by International Human Rights Group Agora and digital rights group Roskomsvoboda stated that the introduction of this law, among a range of other legislative initiatives, shows a fundamental turn in Russian policy on Internet regulation as it is reoriented towards gaining control over objects of infrastructure that have access over user information as well as shaping opportunities to significantly limit the dissemination of information. Similarly, as noted by a report of Human Rights Watch,[108] efforts to increase control over Internet infrastructure like the aforementioned sovereign Runet law, could provide significant restrictions for digital rights in Russia as they intensify extant legislation focusing on content controls through the centralization of control over information infrastructure.

This recent broadening of Internet regulation to include not only content, but also legislation aimed at achieving infrastructural control, is visible in the legislative framework specific to countering terrorist activities online as well. Before 2014, apart from the 2006 law on countering terrorism,[109] the 2002 law on countering extremism[110] and specific parts of the Penal Code of the Russian Federation,[111] laws used to counteract terrorist acts in the information space were mainly aimed at countering the dissemination of terrorist and extremist content, incitements to violence and recruitment. Since the determination of what constitutes extremist content is left rather broad, the prohibition of content inciting enmity and mass disruptions, has been used often as a basis to block content on protests and to pursue legal action against participants.

The first significant piece of legislation focusing on the closer monitoring and blocking of prohibited content is the 2012 resolution of the government of the Russian Federation on the establishment of a register of websites containing forbidden information.[112] From this point on Roskomnadzor[113] had the authority to manage the register of these websites, as well as to require network operators to block them. The provision of this authority to Roskomnadzor was not necessarily aimed at countering terrorism, but came about in the context after the electoral protests in Russia between 2011 and 2012. In 2013 extremist content was explicitly prohibited through an amendment to the law on information,[114] specifically in the context of mass disruptions.

Crucially, this law also contained the provision that websites specifically containing extremist information and information aimed at causing mass disruptions could be blocked within the hour without the need for court intervention or having to inform the owner of the site.[115] From 2011

108 Human Rights Watch. "Russia: Growing Internet Isolation, Control, Censorship", New York, 18 June 2020.

109 Russian Federation. Federal Law N°35-F3, 2006.

110 Russian Federation. "Federal Law N°114-F3 On the Counteraction of Extremist Activities". 25 July 2002. An unofficial translation can be found here.

111 Specifically, articles 205-206, 208, 211, 220, 221, 278, 279, 360, 361 and chapter 28 on crimes in the area of computer information.

112 Russian Federation. "Government Position on the Unified Automated Information System "Unified Register of Domain Names, Indexes of Pages of Sites in the Information and Telecommunication Network "Internet" as Well as Network Addresses, Allowing to Identify Sites in the Information and Telecommunication Network "Internet", Containing Information of Which the Distribution Is Prohibited in the Russian Federation"", 26 October 2012.

113 The Federal Service for Supervision of Communications, Information Technology and Mass Communications.

114 Russian Federation. "Federal Law N°398-F3 on the Introduction of Changes in the Federal Law on "Information, Information Technologies and on the Protection of Information"", 28 December 2013.

115 *Ibid.,* Art. 2.

onwards, accusations of extremism were used often as a tool of political repression.[116] The article of the Penal Code that had become emblematic for this practice, was article 282, which became commonly known as the "law against likes and reposts".[117] The use of the articles in the Penal Code related to extremism had become so prevalent that the number of related convictions had multiplied four times since 2011 – half of which were convictions of youngsters under 25.[118] At the end of 2018 this article was softened which meant that all criminal cases on the basis of this article had to be closed and the sentences given reviewed. In view of this softening, the article was applied less in the course of 2019 as prosecution was diversified through the introduction of new articles to the Penal Code regarding the countering of "fake news", "disrespect to the authorities" and the "incitement of hate".[119]

The recent softening of this article in the Russian Penal Code should be looked at from the perspective of the ongoing broadening of the legislative framework to include infrastructural controls. In the case of legislation aimed at countering terrorism, the so-called "Yarovaya package" of laws constitutes the most emblematic example. Named after its initiator Irina Yarovaya – chairman of the Duma Committee for Security and the Counteraction of Corruption – this legislation consists of:

1. Changes to the Communications law[120]
2. The inclusion of "International Terrorism" into the Russian Penal code[121]

The changes to the Communications Law in particular were met with criticism due to their incursion on users' privacy, since it requires network operators to save date and metadata on all communication and calls during a period of 6 months. Additionally, it required Internet and telecommunication companies to provide information necessary for decoding electronic messages.[122] Public debate on privacy concerns came to a head with the refusal of Telegram to provide information to decode data in electronic messages.[123] The blocking of Telegram led to an increased use of VPNs,[124] which subsequently led to the introduction of a law prohibiting the use of anonymizers and VPNs to access websites containing forbidden content.[125] In addition to this, these services have to subscribe to the Federal State Information System (FGIS), which contains a list of forbidden Internet resources, upload the list of forbidden sites from FGIS and restrict access to them in Russia.'[126]

116 International Human Rights Group Agora. "Internet Freedom 2019: The 'Fortress' Plan", 2 March 2020:11.

117 See Article 282 of the Russian Federation's Penal Code on "The Incitement of Hatred or Enmity as Well as Degradation of Human Dignity", 13 June1996.

118 Kurilova, Anastasia. "Sudebnaya Statistika Voshla v Ekstremistskij Rost" (Court statistics on cases of extremism have gone up), *Kommersant* 68, 19 April 2018.

119 International Human Rights Group Agora, 2020.

120 Russian Federation. "Federal Law N°374-F3 on the Introduction of Changes in the Federal Law "on the Counteraction of Terrorism" and Certain Legislative Acts of the Russian Federation with Regard to Establishing Additional Measures to Combat Terrorism and Ensure Public Security", 6 July 2016. An unofficial translation and analysis of the 'Yarovaya Law' can be found here.

121 Russian Federation. "Federal Law N°375-F3 introducing Amendments to the Criminal Code and Criminal Procedural Code of the Russian Federation in parts Related to the Counter-Terrorism and maintenance of Public Order", 6 July 2016.

122 Russian Federation. Federal Law N°374-F3, 2016: Art. 15 (§3).

123 See Gorbunova, Yulia. "Telegram Loses Free Expression Battle to Russian Authorities", Human Rights Watch, 13 April 2018.

124 Zhukova, Kristina. "VPN Zarabotali Na Blokirovkach" (VPNs Are Profiting from the Blockings), *Kommersant* 85, 21 May 2018.

125 Russian Federation. "Federal Law N°276-F3 on the Introduction of Changes in the Federal Law "On Information, Information Technologies and on the Protection of Information"", 29 July 2017.

126 Bryzgalova, Ekaterina and Ksenia Boletskaya. "Roskomnadzor Reshil Poka Ne Blokirovat VPN-Servisy" (Roskomnadzor Decided to Not Block VPN Services for Now), *Vedomosti,* 26 June 2019.

The law foresees the blocking of these services, if they fail to comply, but in practice Roskomnadzor prefers to issue fines for as long as VPN services do not subscribe to FGIS.[127]. This preference for a policy of fining could be explained by a lack of technical resources. This position was put forward as well by Karen Kazaryan of the Russian Association for Electronic Communications (RAEC) in 2019, who posited that Roskomnadzor has limited options to actually block these services due to a lack of "ready-made technical solutions for this purpose" and the fact that "the law does not yet have corresponding by-laws".[128]

The recent formal unblocking of Telegram in June 2020[129] constitutes another example of the current lack of effectiveness of this package of laws. While the main reason for the decision to unblock Telegram by Roskomnadzor was the "willingness expressed by the founder of Telegram to counter terrorism and extremism",[130] an additional reason was put forward by the Aleksej Volin, Deputy Minister of Digital Development of the Ministry of Communication. At the 2020 Valdaj conference he noted that another reason for the decision was "the impossibility of technical blocking of Telegram"[131]. Alternatively, the emphasis that Roskomnadzor put on the importance of dialogue with Telegram in its statement could also be a sign of increased willingness of Russian authorities to open the door for a more open debate with platforms on this type of legislation.

In spite of its limited application, the impact of the Yarovaya package should not be discounted, as it has arguably laid the basis for a surge of legislation aimed at achieving sovereign control over information infrastructure. In the context of digital rights, this shift in focus seems to imply a shift in policy practice, which consists of the broadening of the set of tools available to achieve control over content dissemination through greater control over the information infrastructure. An example of this is the use of strategic internet outages in times of societal unrest and protests. An important example of this was the 2019 mobile Internet outage in the region of Ingushetia during protests surrounding a controversial border deal with Chechnya.[132] The outage was deemed legal by the Magassky District Court of Ingushetia on the basis of article 64 of the Communications law. This article – which was introduced into the communications law on the basis of the 2006 counterterrorism law[133] – provides the FSB with the possibility of requiring network operators to shut down their services. In the case of Ingushetia, the reason put forward for requiring these outages was also the existence of a potential threat of terrorist activities.[134]

127 *Ibid.*

128 Kuranov, Ivan. "Blokirovka VPN-Servisov v Rossii Okazalas Nevostrebovannoj" (Blocking VPN Services in Russia Turned out to Not Be Required), RBC, 20 February 2018.

129 Sherman, Justin. "What's behind Russia's decision to ditch its ban on Telegram?", Atlantic Council, 26 June 2020.

130 Federal Service For Supervision In The Sphere Of Communications, Information Technology And Mass Media. "O messendzhere Telegram" (On the messenger Telegram), *Roskomnadzor,* 18 June 2020.

131 See Aleksej Volin's contribution at the Valdaj Club's online discussion "Novyj mirovoj politicheskij narratives: stil' i slog" (New global political narratives: style and language), minutes 27:00-30:00 (in Russian).

132 RFE/RL's North Caucasus Service. "Ingush activists under pressure after protests over Chechnya border deal", *RadioFreeEurope,* 3 April 2019.

133 Russian Federation, Federal Law N°375-F3, 2006.

134 Edwards, Maxim. "Who turned off Moscow's internet during recent protests?", *Global Voices,* 9 August 2019.

While the language of cyber terrorism itself is not used specifically in Russia to push through these legislative changes, the potential threat of terrorist activities does seem to form a fertile ground for the imposition of government controls on the online information space. In particular ongoing efforts to increase sovereign control over Internet infrastructure have gained a push from anti-terrorism initiatives like the Yarovaya package. The introduction of measures of Internet regulation banking on greater control over information infrastructure is having a significant impact on how Russia implements these controls in practice. Whereas previous to 2018, the focus lay heavily on the use of content controls to deter opposition activities, current efforts towards achieving infrastructural control seem to give way to the use of strategic internet outages in addition to the targeted blocking of information.

6. France: issues of form and substance in the national strategy of terrorist threat anticipation in cyberspace

Rebecca Mignot-Mahdavi

Since the 2010s, and even more intensely since the Paris attacks of 2015, France built a heavy legal arsenal to track and counter jihadist communications and propaganda online, and more generally hate speech.[135] This occurred by reinforcing the mandate and power of intelligence services, but also through the organisation of ever closer collaborations between law enforcement agencies and digital platforms. The goal of this national strategy was to ensure (i) that law enforcement and intelligence agencies would receive more information so to be more able to anticipate threats, and (ii) that communications and expressions considered "undesirable" – to borrow President Macron's UNESCO speech terminology[136] – are excluded from the web.

This closer union between tech companies and state authorities is in line with the mandate of the EU Internet Forum, an initiative launched in 2015, to bring together governments, Europol and technology companies to counter terrorist content and hate speech online.[137] The Global Internet Forum to Counter Terrorism (GIFCT), formed in 2017, is yet another example not only of the growing importance of digital platforms in preventing terrorists from exploiting digital platforms,[138] but also of the essential role played by France in fostering this cooperation. France also emerged as a driving force of the Christchurch Call which provided the stimulus for the creation of the GIFCT[139] and is one of the few state members of the GIFCT Independent Advisory Committee (IAC).[140]

135 It should be emphasized at the outset that France's constitutional regime is a semi-presidential one. It is hence characterized by a strong Executive, a Parliament composed of a strong presidential majority and a very 'weak' opposition, especially since Parliamentary and Presidential elections have been synchronized in 2000 (with the reduction of the presidential mandate from seven to five years, thus aligning itself with the parliamentarians' mandate). Because of this constitutional nature, legislation can really be understood as materializing governmental policies.

136 Élisée. "Speech By M. Emmanuel Macron, President Of The Republic At The Internet Governance Forum", UNESCO, Paris, 12 November 2018.

137 The creation of the forum was one of the main elements of The European Agenda on Security. On this, see European Commission. "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions", Strasbourg, 28 April 2015: 13-16.

138 Founded by Facebook, Microsoft, Twitter, and YouTube, the GIFCT's working groups and diverse programs involve industry, government and civil society. Further information on the GIFCT can be found on the official website.

139 The Christchurch Call was adopted by France, New Zealand, Canada, Ireland, Jordan, Norway, the UK, Senegal, Indonesia, the European Commission, and a number of tech companies (Amazon, Facebook, Google Microsoft, Qwant, Twitter, YouTube, and DailyMotion).

140 Note that no other EU member state is a member of the IAC of the GIFCT. The European Commission, however, is a member of the IAC.

However, the French Supreme Court *(Conseil Constitutionnel)* recently considered that the Macron government went too far in its pursuit of online surveillance and speech regulation. With a new law against online hatred *(Loi Avia contre la haine en ligne),* the Macron government wanted to implement a cooperative regulation that would require tech firms to spot, among other types of hate speech, terrorist communications online and delete them within twenty-four hours of publication.[141] By a decision of 18 June 2020, French supreme judges considered the core provisions of this law unconstitutional on the basis of Article 11 of the Declaration of the Rights of Man and of Citizens of 1789 (which has constitutional value). The supreme judges considered that (i) having the sole administration, (ii) without judicial review, (iii) determine the illicit character of the contentious contents without necessarily having "manifest" elements, (iv) and leading to their deletion, (v) within a very short period of time (24 hours), would disproportionately restrict freedom of expression.[142]

As is well known, tech companies have taken the lead and made increasing efforts over the past years to remove and block terrorist content from their platforms, including by using artificial intelligence.[143] The provisions of the above-mentioned Loi Avia censored by the Constitutional Council were very much in line with the German Network Enforcement Act (NetzDG), adopted in 2017, which among other things provides for a fine of up to €50 million if a platform systemically fails to delete illegal content.[144] The shared Franco-German trajectory is reflected in the joint letter addressed in April 2018 to the European Commission by the French and German Interior Ministers, in which they clearly stated that these laws aimed at generalizing to the entire web the censorship mechanisms developed by Facebook and Google to counter terrorism.[145] In their letter, the French and German ministers expressed their inclination for the creation of a European legislation to give a uniform framework to the foreseen private-public collaborations, reflecting again the two countries' leading role in developing the EU initiative for the regulation of online content.

The prominent role that France has taken on in the fight against terrorism at the European and international levels as web and speech regulator is at odds with its tradition of intense (judicial) protection of freedom of expression.[146] Already in the physical world, the most recent French laws

141 French Republic. "Loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet", 24 June 2020.

142 Constitutional Council of the French Republic. "Décision du Conseil constitutionnel n° 2020-801 DC", 18 June 2020.

143 Facebook. "Partnering to Help Curb Spread of Online Terrorist Content", Facebook News, 5 December 2016; Bickert, Monika and Brian Fishman. "Hard questions: how we counter terrorism", Facebook News, 15 June 2017; Tech Against Terrorism. "UK launch of tech against terrorism at Chatham House", Chatham House, 12 July 2017; Bickert, Monika and Brian Fishman. "Hard Questions: How Effective Is Technology in Keeping Terrorists off Facebook?", Facebook News, 23 April 2018; Twitter Inc. "Combating violent extremism", Twitter blog, 5 February 2016; Twitter Inc. "New data, new insights: Twitter's latest #Transparency report", Twitter Public Policy, 19 September 2017; Twitter Inc. "Expanding and building #TwitterTransparency", Twitter Public Policy, 5 April 2018. For a socio-legal analysis of this practice, please see Macdonald, Stuart, Sara Giro Correia, and Amy-Louise Watkin. "Regulating terrorist content on social media: automation and the rule of law", *International Journal of Law in Context* 15/2, (2019): 183-197.

144 German Bundestag. "Article 1 Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act)", 1 September 2017.

145 Letter of 2 April 2018, addressed by Interior Ministers of Germany (Horst Seehofer) and France (Gérard Collomb) to European Commission's Vice-President Andrus Ansip and Commissioners Mariya Gabriel, Vera Jourová, Dimitris Avramopoulos, and Julian King.

146 The tradition mentioned here is encapsulated in the Law on the Freedom of the Press of 29 July 1881, which is the founding text of freedom of expression in France, adopted in reaction to the Napoleonian criminal code. It provides that, in principle, any matter related to freedom of expression is subject to the press code and not to the criminal code.

were used to severely sanction speech glorifying terrorism.[147] Applying such rules to the cyber world makes the occasions of censorship even more numerous – even more so when surveillance and speech regulation are automatized. As a result of the application of these new laws to communications on the web, freedom of expression is arguably even more at peril.

As the digital revolution has just begun and, with it, possibilities for public expression to flourish on the internet have increased, speech regulation and digital surveillance grow exponentially. Currently in France, anyone can observe the plethora of freedom-restrictive counter-terrorism measures such as the criminalization of the "apology/glorification of terrorism", the increase of the severity of sanctions for such acts,[148] the extensive discretionary power given to administrative authorities to block websites that glorify terrorism or to automatically intercept digital data flows, as well as other intrusive surveillance measures and speech regulation practices.[149] These measures raise three key substantial concerns that addressed in this contribution: extensive administrative discretion, lack of legal clarity and limited judicial review. Besides their problematic nature in substance, the way in which the government pushed for the adoption of these measures is also problematic in a democratic society. The government made the choice not to emphasize on its understanding of the internet as a risk enhancing terrain in the pieces of proposed legislation submitted to Parliament. It is likely that policymakers feared to trigger parliamentary and public debate on their preventive approach to terrorism.

Issue of Form: Still Waters Run Deep

Parliamentary discussions on the 2015 Intelligence Law – dedicated to organizing and facilitating surveillance conducted by intelligence personnel to prevent terrorism – started with the opening remarks by the then-Prime Minister Manuel Valls underlining the unprecedented risk posed by cyber-threats.[150] On this occasion, he referred to the hacking of TV5 Monde, conducted earlier in the same year by a terrorist group who managed to express support for the Islamic State for several hours of broadcasting. Deputies from all parties expressed their understanding of threatening technological evolutions and cyber-threats, including some that can put at risk vital infrastructures and "public liberties" (with reference to the TV5 Monde cyberattack).[151]

147 For instance, a train passenger who – in the midst of an altercation with the railway agents – told them "Allah Akbar (...) If I had a bomb I would make everything explode" was sentenced to imprisonment (see Chabaud Corinne. "Apologie du terrorisme : quand la justice s'emballe", *La Vie,* 27 January 2015). Similar charges were given to a man who – arrested for drink-driving – yelled "There should be more people like the Kouachi brothers. I hope you will be next" to the police officers; and to a man who shouted to police officers "They killed Charlie and I had a good laugh" (see Henry, Michel. "Apologie du terrorisme: la justice cogne ferme", *Libération,* 14 January 2015).

148 French Republic. "LOI n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme", 13 November 2014.

149 French Republic. "LOI n° 2012-1432 du 21 décembre 2012 relative à la sécurité et à la lutte contre le terrorisme", 21 December 2012; French Republic. "LOI n° 2015-912 du 24 juillet 2015 relative au renseignement"; French Republic. "LOI n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale", 3 June 2016; French Republic. "LOI n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme", 30 October 2017.

150 Manuel Valls: "Si l'enquête est toujours en cours concernant TV5 Monde, l'acte a été revendiqué par un mouvement terroriste. C'est un fait : les attaquants étaient présents dans le système d'administration du réseau depuis plusieurs semaines. Cette agression est emblématique d'une nouvelle forme de menaces : les cyber-menaces. Si la société numérique est porteuse de nombreuses promesses, elle présente aussi des vulnérabilités inédites". In National Assembly of the French Republic. "Transcript of the discussions on the Proposed Intelligence Act", Session of 13 April 2015.

151 *Ibid.*

However, despite political consensus on the fact that the internet constitutes a catalyst for disruptive terrorist threats, the Parliament decided not to make explicit reference to cyber threats and to internet-based threat anticipation. Left MP Jeanine Dubié presented a request to amend the proposed text and to use the term "cyber criminality" *(cybercriminalité)* and not only "criminality" *(criminalité)*. This proposition aimed to clarify the *raison d'être* of the text: to prevent cyber criminality. Both the representative of government who was present that day, Christiane Taubira, and the representative of the parliamentary commission Jean-Jacques Urvoas, expressed their negative opinion on this request. They were concerned that the use of "cyber" in this text would lead, *a contrario,* to exclude cyber criminality from texts that only refer to criminality.[152] The draft amendment was not taken on board.

As a result, the cyber elements would remain 'in the shadows', even if they are presented and accepted as key drivers of the French security policy. The specific security measures implemented by counter-terrorism legislation are in themselves revealing of the prominent importance given to the internet, not only as a risk enhancer terrain but also as one that allows threat anticipation. Most measures adopted at the end of the parliamentary process aim at facilitating surveillance, action which can be defined as that of watching (in French, *"veiller sur"*) a person or an operation over time; in order to track and address the development of those who are monitored. As such, surveillance is inherently preventive.[153] In the absence of emphasis on the cyber element in the French counter-terrorism legislation, the preventive turn of the policy that the cyber world allows goes unnoticed.

Yet, the preventive nature of the French counter-terrorism policy leads, as we will further explore below, to intrusive practices. Speech – regardless of the recent failure of the government to pass the most important restrictions with the Loi Avia – remains monitored through the framework implemented by other existing legislations. In particular, the 2015 Intelligence Law aims to prevent threats on the internet through enhanced surveillance practices and, even more precisely, through the automatic processing of personal data. This automatic processing works through an algorithmic system that infers from certain elements of information characterized as "suspicious" (based on criteria that are unknown to the public and remain unaddressed/undefined by courts or any other independent authority) that an individual or an activity is potentially threatening.[154] Provisions of the 2016 Law "reinforcing the means to fight against terrorism and the efficiency of criminal proceedings" also legalize the recourse to IMSI-catching technology, allowing to capture, thanks to a fake antenna, all connection data of any person detaining an electronic device in a defined geographical area.[155] In other words, recent legislation normalizes the possibility of systematic, generalized, and vaguely-constrained practices of data collection.

152 *Ibid.,* amendment proposal n°162. This amendment was discussed but ultimately not adopted. The Assembly agreed that cyber-criminality is a form of criminality but "mentioning cyber criminality would create the risk of having this form of criminality understood as excluded when only "criminality" is referred to".

153 See section on surveillance in Cornu, Gérard. *Vocabulaire juridique,* Presses Universitaires de France, 2020.

154 The 2015 Law creates a new article in the Code for domestic security (Code de la sécurité intérieure) that allows, for the sole purpose of *preventing* terrorism, the recourse to such methods.

155 French Republic. LOI n° 2016-731, Art. 2. For more information on the Parliamentary discussions preceding the adoption of the law, please see the legislative dossier here.

Parliamentary opposition to these extended surveillance practices – such as the recurrence to algorithmic detection systems – has been bland. Isabelle Attard, a Green MP, criticized the law as "the information obtained is extremely rich as it allows the authorities to know with whom a suspicious person entered in contact, how many times per day or per week, how long their conversations lasted, what is the content of these conversations, what websites are then consulted by all participants".[156] In response to this critique, the parliamentary majority argued that the internet is both a catalyst for the preparation of terrorist acts as well as a unique resource for anticipating threats, and these opportunities should be taken.[157]

Overall, very few attempts were made to push back against the intrusive nature of surveillance practices, and it was sufficient for the governmental majority to succinctly emphasize on how cyberspace exacerbates threats to get the law adopted. The government's choice to remain ambiguous on its counter terrorism policy goals is not surprising.[158] To purposefully avoid meaningful parliamentary debates and societal conversations on the limits that governmental security practices should know to preserve human rights is problematic in a rule-governed society.

Issues of Substance: Intrusive and Unchecked Eye in the Web

The intrusive surveillance methods adopted by France in recent years put fundamental rights at risk. Three core concerns deserve attention. First, the criteria set by the 2015 Intelligence Law that are supposed to help identify legitimate surveillance targets are so vague (or unknown, or automatized) and open to discretion that they barely perform any constraining function. In an opinion of 16 April 2015, the French National Consultative Commission on Human Rights ('CNCDH') raised awareness and expressed concerns on the wide scope of the metadata that can be collected as well as on the vagueness of the criteria used to identify surveillance targets: persons "previously identified as posing a threat". According to the CNCDH, these criteria imply a diagnosis of dangerousness and a prognosis of future action based on hazardous definitions. In such conditions, the scope *ratione personae* of the collection of data is potentially very large: the anticipatory logic of the measure could potentially put a large amount of people under surveillance. This can affect privacy rights as well as freedom of expression in a possibly extensive manner.

Second, the pre-emptive emphasis put in all recent French counter-terrorism laws not only implies that a wide number of people are targeted by such intrusion. It also allows surveillance practices to escape substantial judicial review and leaves the relevant administrative authorities unchecked. Yet, the judiciary's role is precisely to protect basic rights and freedoms of individuals, including

156 Statement of Isabelle Attard (Green Group) at the National Assembly of the French Republic. "Transcript of the discussions on the Proposed Intelligence Act", Session of 13 April 2015.

157 Statement of Jean-Yves le Drian (former Minister of the Interior) at the National Assembly of the French Republic. "Transcript of the discussions on the Proposed Intelligence Act", Session of 13 April 2015.

158 This choice is not specific to domestic counter-terrorism practices. France's extraterritorial counter-terrorism policy is also in many aspects indirect and implicit. On this, please see Mignot-Mahdavi, Rebecca. "Le Silence des Agneaux: France's War Against 'Jihadist Groups' and Associated Legal Rationale", International Centre for Counter-Terrorism (ICCT), The Hague, 15 May 2020.

from administrative practices that are illegitimately intrusive.[159] The understandable objective to anticipate terrorist threats should not lead to neglecting the crucial role of the judiciary in exercising control over measures that potentially affect human rights and to check if administrative intrusion is excessive.[160] This is especially true that no valid reason justifies to circumvent judicial review in this case. Indeed, these surveillance measures are taken in *anticipation* of threats. As such, there is no urgency to adopt such measures. Yet, only urgency could justify the rapid recourse to administrative decision making. In fact, the more prospective the administrative measure is, the lesser justifiable it is to circumvent judicial review.

Third, the requirement that intrusion in private life is only permissible if a "legitimate interest" justifies it, is very imprecise. Even if limitations to individual rights could be accepted on the basis of national security interests, the law has to use sufficiently clear terms to indicate under which circumstances and conditions the public authority is allowed to secretly intrude into people's private lives. When neither the type of information nor the categories of persons who are likely to be the object of such surveillance and data collection measures are mentioned in the law, the right to private life can be considered violated.[161]

According to the CNCDH, the characterization of a "legitimate interest" is for this reason in blatant violation of Article 8 of the European Convention on Human Rights protecting the right to respect for private and family life. To escape this criticism, the government argued that it is wrong to consider that algorithmic surveillance is massive as, it contends, the algorithm exclusively detects the individuals who adopt the cyber behavior preidentified as suspicious (as "resembling the communication patterns of terrorists"). This argument, however, completely turns a blind eye on the fact that in order to detect, the system analyses all available data and can thus, without doubt, be characterized as a mass surveillance program. In addition, the French government underlines that such systems are only deployed to prevent terrorism, again ignoring that both pre-emption and terrorism potentially lead to open-ended practices.

Against this background, some scholars have expressed concerns about the habit of French public authorities to ignore the right to privacy and freedom of expression when adopting measures to counter terrorism.[162] These measures run counter to the case-law of the European Court of Human Rights and the European Court of Justice on these issues.[163] Even if for now these courts have not

159 For a similar position, please see Mallet-Poujol, Nathalie. "Introduction", *LEGICOM* 2/57, (2016): 55-56; Monfort, Jean-Yves. "Le blocage administratif des sites prévu dans la loi du 13 novembre 2014 de lutte contre le terrorisme", *LEGICOM* 2/57, (2016): 69-74; Salzer, Anne. "La loi sur le renseignement : surveillance et interceptions techniques", *LEGICOM* 2/57, (2016): 75-80. Salzer powerfully declares that the judiciary has disappeared from surveillance practices.

160 Boutin, Berenice. "Administrative Measures against Foreign Fighters: In Search of Limits and Safeguards", International Centre for Counter-Terrorism (ICCT), The Hague, December 2016, (p. 4): "The same goes for references to non-judicial measures: although the involvement of the judiciary in the application and review of administrative measures is often limited, the terms such as non-judicial measures can wrongly imply that no judge is involved at all."

161 Cases references: "Association Confraternelle De La Presse Judiciaire V. France Et 11 Autres Requêtes", (nos. 49526/15, 49615/15, 49616/15, 49617/15, 49618/15, 49619/15, 49620/15, 49621/15, 55058/15, 55061/15, 59602/15 and 59621/15).

162 Parizot, Raphaële. "Surveiller et prévenir… à quel prix ? – Loi n°2015-912 du 24 juillet 2015 relative au renseignement", *La Semaine Juridique Edition Générale* 41, (2015): 1816-1824; Lazerges, Christine and Hervé Henrion-Stoffel. "Politique criminelle, renseignement et droits de l'homme. A propos de la loi du 24 juillet 2015 relative au renseignement", *Dalloz Revue de science criminelle et de droit pénal comparé* 3, (2015): 761-775; Gras, Frédéric. "Des « lois scélérates » aux premières applications par les tribunaux du délit d'apologie du terrorisme", *LEGICOM* 2/57, (2016): 57-67.

163 Gautron, Virginie and David Monniaux. "De la surveillance secrète à la prédiction des risques: les dérives du fichage dans le champ de la lutte contre le terrorisme", *Archives de politique criminelle* 1/38, (2016): 123-135.

addressed the French case specifically, their decisions have been consistent and clear with regards to those large-scale surveillance practices whose criteria are not made public.[164] Applications to the European Court of Human Rights were communicated to the French Government on 26 April 2017 (lodged by lawyers and journalists) concerning the French Intelligence Act of 24 July 2015. The Court gave notice of the applications to the French Government and put questions to the parties under Articles 8 (right to respect for private life and correspondence), 10 (freedom of expression) and 13 (right to an effective remedy) of the Convention.[165]

Conclusions

France did not make explicit that its counter-terrorism policy is based on the ideas that internet (i) catalyzes risks and (ii) must be used to intensify surveillance practices. This choice might have made the law and policy making process easier: it somehow ensured that no vivid public discussion would take place on the specificities of surveillance and speech regulation on the web (i.e. the anticipatory turn that it facilitates).[166] The preventive character of threat monitoring also gave the upper hand to administrative authorities and made sure that judicial control would not be exercised.

In the meantime, we have seen that information gathering methods have increased in number and scope throughout the adoption of successive laws without ever seeking for popular or judicial legitimacy, hindering debates and reflections in the media. These issues of form and substance appear to be quite problematic in a democratic, rule-governed society and potentially very harmful for social cohesion and institutional trust in the long run. In addition to taking into consideration the above-mentioned elements related to potential human rights abuses when shaping surveillance practices, the implicit importance given to cyber elements in crafting counter-terrorism policy should be brought to light and made explicit.

164 European Court of Justice (ECJ). "Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd et al., EU:C:2014:238"; European Court of Human Rights (ECHR). "Case Of Shimovolos V. Russia", no. 30194/09, 21 June 2011; ECHR. "Dimitrov-Kazakov c/ Bulgaria", no. 11379/03, 10 February 2011.

165 Similar applications are pending – Follorou v. France (no. 30635/17) and Johannes v. France (no. 30636/17) – and were communicated to the French Government on 4 July 2017.

166 State officials justify the lack of transparency on the basis of article 26-III of the French Data Protection Act accepting that data collection systems and surveillance practices are not publicly detailed when they pursue state security. Article 44 IV of the Data Protection Act also removes some information banks from the control of the National Commission for Information Technology and Civil Liberties (CNIL) when they concern national security. Even when the CNIL has access, the opinions it formulates are not binding and can be disregarded by the Prime Minister.

7. European Union: the narrative implications of conceptualizing cyber terrorism as a threat

Stef Wittendorp

Terrorism, cyber terrorism, and cybercrime at the EU level

It is often quipped that cyber terrorism is more debated than actually occurring. This contribution argues that even these debates about cyber terrorism already produce actual consequences for the regulation of cyberspace and has implications for both civil liberties and cyber security. By focusing on the European Union (EU) level, this contribution explores two conceptualizations of cyber terrorism: (1) as the terrorists' use of the internet and (2) as terror through digital disruption for political purposes. These different conceptualizations translate into different estimations of what kind of threat cyber terrorism is and impacts what count as legitimate activities in cyberspace. This results in a reflection on cyber terrorism as a *narrative or discourse* for assessing and regulating risks and (il)legal activities in cyberspace.

Since 2002, the EU has built up an extensive legal repertoire about terrorist offences, especially when compared to legal instruments dealing with cybercrime and cyber security. EU legislation on terrorism has criminalized a broad range of activities, including membership, public provocation, recruitment, providing and receiving training, travelling, the facilitation or organization of travel and financing.[167] Cyber terrorism, however, is not a legal concept at the EU level. The term does appear in reports and documents, but mostly in an incidental manner. The most extensive engagement with the digital activities of terrorists can be found in Europol's Internet Organised Crime Threat Assessment (IOCTA), an annual review of developments with regard to cybercrime. The report touches on the two concepts of cyber terrorism, but predominantly discusses the activities of terrorists in cyberspace: the distribution of propaganda, recruitment efforts and the use of encryption. Cyberattacks by terrorists aimed at disruption are discussed, but mainly as something these actors either have a limited capacity for or as a future concern.

The dominant manner at the EU level of characterizing illegal activities in cyberspace is with the term *cybercrime*. For instance, the IOCTA is organized around the notion of cybercrime and this report is produced by Europol's European Cybercrime centre (EC3). Relevant policy documents such as the EU's cyber security strategy or the European Agenda on Security primarily draw on the terminology of cybercrime, with no or only passing reference to cyber terrorism.[168] Key legal instruments

167 See Council of the European Union and European Parliament. "Directive (EU) 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,* L 88.

168 European Commission and High Representative for the Common Foreign and Security Policy. "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", Brussels, 7 February 2013; European Commission. "The European Agenda on Security", Strasbourg, 28 April 2015.

criminalizing cyber activities such as Directive 2013/40/EU, the NIS Directive and the Cybersecurity act are justified in relation to cybercrime, not cyber terrorism.[169] These instruments refer to the damaging and disrupting of digital infrastructure with the language of 'attacks', 'incidents' and 'threats', not 'terror', the latter being a more narrow category pointing to specific means of disruption and/or the effects thereof. For instance, 'cyber threats' is given as a generic definition: 'any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact' networks, information systems or their users.[170]

Cyber terrorism as the terrorist use of the internet

The EU seems to understand cyber terrorism mainly as the use of digital infrastructure by terrorists for distributing extremist content, engaging in recruitment and communicating via encrypted means. That the EU seeks to regulate online activities of terrorists is not surprising: society has become more digitized; terrorists have not remained immune to this development and new actors (hosting service providers) have emerged as facilitators and regulators of digital activities requiring clarification of roles and responsibilities. However, scrutiny of policies for addressing the terrorists' use of the internet – most prominently the European Commission's proposal on tackling online terrorist content – remain vital.[171] Civil rights groups point to the broad scope of material that can be earmarked as terrorist content and the negative implications for freedom of speech that follows from this.[172]

Notwithstanding the digitization of society and the need for regulating against its undesirable aspects, it remains important to interrogate the security imperative informing proposals such as that of the Commission. The proposals' claims to the 'instrumental' nature of terrorists' online activities in committing attacks and the easy accessibility of online terrorist content , suggest the online domain as an all important dimension in countering terrorism.[173] However, scholars caution against linear and causal understandings of the influence of the internet on terrorist motivations and operations. Gill et al. point to the situated and interactive relation between perpetrators of violence and their use of the internet. They found virtually no indication of the internet as the sole pathway of involvement into terrorist activities. Face-to-face dynamics remain the most important dimension for explaining why

169 European Parliament and Council of the European Union. "Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on Attacks against Information Systems and Replacing Council Framework Decision 2005/222/JHA", *Official Journal of the European Union,* L 218; European Parliament and Council of the European Union. "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union", *Official Journal of the European Union,* L 194; European Parliament and Council of the European Union. "Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) 526/2013 (Cybersecurity Act)", *Official Journal of the European Union,* L 151.

170 European Parliament and Council of the European Union. "Cybersecurity Act," 2013: 64.

171 'Content' is understood to mean contributing (directly or indirectly) to the advocating of committing a terrorist offence, soliciting others to join a terrorist group, providing instructions on explosives, weapons or dangerous substances, depicting the commission of a terrorist offence, dissemination of terrorist content online, see European Commission. "Proposal for a Regulation of the European Parliament and of the Council on Preventing the Dissemination of Terrorist Content Online", European Parliamentary Research Service, 12 September 2018.

172 van Hoboken, Joris. "The Proposed EU Terrorism Content Regulation: Analysis and Recommendations with Respect to Freedom of Expression Implications", Transatlantic Working Group, 3 May 2019; Committee to Protect Journalists. "EU Online Terrorist Content Legislation Risks Undermining Press Freedom", 11 March 2020.

173 European Commission. "Proposal for a Regulation of the European Parliament and of the Council on Preventing the Dissemination of Terrorist Content Online", 2020: 1.

and how someone turns to violence. Gill et al. thus characterize '[v]iolent radicalization (...) as cyber-enabled rather than as cyber-dependent while underlining that enabling factors differ from case to case depending on need (...) and circumstance'.[174]

The security imperative informing the Commission proposal requires scrutiny for two additional reasons. First, justifying policies on the basis of urgency and vital importance in order to get a grip on the terrorist problem might reduce the scope of critical inquiry by prioritizing the speed of legislative action over substantive questions of feasibility, digital rights and civil liberties.[175] Second, the security imperative raises expectations about the ability of actors to restrict and regulate the terrorists' use of the internet that these actors might not be able to meet in the first place. This sets the stage for a downward regulative spiral whereby the failure to regulate effectively fuels the need for more regulation while leaving the underlying questions of feasibility and problem definition untouched.[176]

Cyber terrorism as the disruption of the digital infrastructure

The second meaning of cyber terrorism (attacking digital infrastructure in order to cause wide-scale societal disruption) occupies a more marginal place in EU discourse compared to the terrorists' use of the internet. The disruption of digital infrastructure in order to cause terror for political purposes is discussed primarily as a potential, future scenario rather than an actual phenomenon. Whether to take cyber terrorism seriously is thus made dependent upon the availability of empirical data that proves or might prove its existence. However, this overlooks how cyber terrorism functions as a discourse or narrative shaping what, when and how to regulate cyber space.

Cyber terrorism as a discourse means that its existence is not inherent to the disruptive cyber act itself, but whether responsible actors decide to treat the incident as cyber terrorism and whether such an understanding is adopted by other involved actors. It is not hard to think of a scenario where a ransom- or malware attack blocks access to valuable data on a large scale (e.g. by targeting a banking app) and ends up terrorizing a population or at least segments thereof. In particular when such acts are accompanied by political demands it would fulfil the conditions for interpreting the attack as a case of terrorism: the use of terror and the effects thereof in terms of terrorizing a population and/or government.

More importantly is perhaps the normative perspective, the question of whether cyber terrorism should be welcomed as a concept for framing illicit activities in cyber space. After all, there is no lack of concepts or instruments for making sense of and responding to illegality in cyber space. The EU's counter-terrorism legislation has a broad character, including the criminalizing of activities conducted in preparation for the committing of the actual violent deed. This covers activities conducted in the digital domain such as recruitment, financing and the organization and facilitation of travel for terrorist purposes. Besides, the legal framework on cybercrime offers terminology for analysing and thus understanding illicit cyber activities. Even this instrument was criticized by the European

174 Gill, Paul, Emily Corner, Maura Conway, Amy Thornton, Mia Bloom, and John Horgan. "Terrorist use of the Internet by the numbers: Quantifying behaviors, patterns, and processes", *Criminology & Public Policy* 16/1, (2017): 99-117.

175 Buzan, Barry, Ole Wæver, Ole Wæver, and Jaap De Wilde. *Security: A new framework for analysis.* Lynne Rienner Publishers, 1998: 23-26.

176 Wittendorp, Stef. "Conducting Government: Governmentality, Monitoring and EU Counter-Terrorism", *Global Society* 30/3, (2016): 481-82.

Parliament for over-criminalizing particular cyber activities.[177] Any broad use of cyber terrorism might therefore negatively impinge on an already ambiguous boundary between legal and illegal cyber activities. Tanczer is critical of the blurring of boundaries between cyber terrorism and hacktivism. The latter being defined as disruptive cyber activities for the benefit of society rather than the former's terrorizing thereof.[178]

Another consequence of the discourse on cyber terrorism relates to the securitization of cyber space: the framing of the digital as a domain of proliferating risks and threats. Terrorism, generally understood as a phenomenon of low probability but of high impact, induces to think about cyber activities in terms of anxieties, suspicions, threats and risks quite disproportionate to the probability of their occurrence. Cyber terrorism then, contributes to the normalization and institutionalization of thinking about exceptional events (large-scale disruptions) in cyberspace.[179] The effect is that worst-case scenario thinking might unduly reduce the space for debating everyday and routinized cyber mishaps, accidents and/or breakdowns. Debating cyber terrorism as a potential scenario with limited empirical validation is not merely a theoretical or academic exercise. It produces real effects: the notion of cyber terrorism informs and shapes political and societal debates of when, where and how to regulate cyberspace by suggesting the specter of the worst-case.

Conclusions

The meaning of cyber terrorism is not self-evident and has consequences regardless of its actual occurrence. Cyber terrorism as referring to terrorists' use of the internet for recruitment, organization and ideological dissemination or as digital disruption in order to terrorize a population or government in order to achieve a political program leads to different estimations in terms of what kind of threat there is and what should be done about it. The former as the digital extension of a known phenomenon (terrorism), the latter as an altogether different type of activity. Underlying these considerations is cyber terrorism as a narrative or discourse that, through the very act of debating the potentiality of such cyberattacks, is shaping political and policy discussions, even in the absence of 'actual' – empirically verifiable – acts of cyber terrorism. Narratives on cyber terrorism are therefore not innocent, but provide ways of framing activities as illicit in cyber space and registers of justification for intervening in cyber space. These narratives can (a) contribute to a blurring of the divide between legitimate and illegitimate activities in cyber space, (b) have negative consequences for civil liberties by imposing further restrictions on freedom of speech and expression without (c) necessarily offering tangible prospects and benefits in terms of providing better protection against threats and risks in cyberspace.

177 European Parliament and Council of the European Union. "Directive 2013/40/EU"; For the critique, see Fahey, Elaine. "The EU's Cybercrime and Cyber-Security Rule-Making: Mapping the Internal and External Dimensions of EU Security", *European Journal of Risk Regulation* 5/1, (2014): 52.

178 Tanczer, Leonie Marie. "The Terrorist - Hacker/Hacktivist Distinction: An Investigation of Self-Identified Hackers and Hacktivists", in *Terrorists' Use of the Internet,* (2017): 77-92.

179 Dunn Cavelty, Myriam. "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse", *International Studies Review* 15/1 (2013): 118; On speculative thinking, see also De Goede, Marieke. "Beyond Risk: Premediation and the Post-9/11 Security Imagination", *Security Dialogue* 39/2-3, (2008): 155-76.

Authors

Fabio Cristiano is postdoctoral researcher and lecturer in the Institute of Security and Global Affairs (ISGA) and a fellow of The Hague Program for Cyber Norms at Leiden University. His research broadly lies at the intersection of critical security studies and international relations theory, with a specific interest for international cyber security and conflicts. Prior to joining Leiden University, Fabio has worked as doctoral researcher and lecturer at Lund University, consultant at the Swedish International Development Agency and the Muslim Council of Britain, editor for Oxford University Press, and lecturer for the government initiative 'AI Competence for Sweden'.

Dennis Broeders is associate professor of security and technology and senior fellow of The Hague Program for Cyber Norm at the Institute of Security and Global Affairs of Leiden University, the Netherlands. His research and teaching broadly focuses on the interaction between security, technology and policy, with a specific interest in international cyber security governance. He is the author of the book *The public Core of the Internet* (2015). He currently also serves as a member of the Dutch delegation to the UN Group of Governmental Experts on international information security (2019-2021) as an academic advisor.

Daan Weggemans is program director of the BA in Security Studies and a researcher at the Institute of Security and Global Affairs (ISGA) at Leiden University/Campus The Hague. He is also a Research Fellow at the International Centre for Counter-Terrorism (ICCT). Earlier research focused on processes of (de)radicalization and re-integration, the radicalization and preparatory processes of Foreign Fighters and contemporary security technologies. He has been an expert witness in various court cases and interviewed dozens of security professionals and (former) violent extremists and their families.

Krisztina Huszti-Orban is a research fellow at the Human Rights Center at the University of Minnesota Law School and senior legal advisor to the United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism. Her background as a practitioner and academic is in international law and security policies, with particular focus on counter-terrorism. She has previously worked with international and regional organizations including the Office of the United Nations High Commissioner for Human Rights and the European Court of Human Rights as well as academia.

Gareth Mott is lecturer in Security and Intelligence in the School of Politics and International Relations at the University of Kent's Rutherford College. His research specializes in the interchange between technology and software and its socio-political implications. He has published on cyberterrorism, peer-to-peer technology and extremist message dissemination, and the role of 'identity' in the security politics of cyberspace. He convenes a module entitled 'Governance and War in Cyberspace'. He is a member of the Institute of Advanced Studies in Cyber Security and Conflict and is a keen advocate of a 'big tent' approach to the interdisciplinary researching and teaching of cyberspace politics.

Siodhbhra Parkin is China program manager at the Global Network for Public Interest Law, where she specializes in civil society engagement and legal advocacy issues. She was previously a Fellow at the Yale Law School Paul Tsai China Center, where she worked on domestic violence and LGBT rights programming. Before that, she was a Program Officer at the American Bar Association Rule of Law Initiative in Beijing. Parkin holds advanced degrees from Harvard University, the London School of Economics and Political Science, and the Renmin University of China. She is also the Director of the Serica Initiative, the newly established nonprofit arm of SupChina.

Eva Claessen is doctoral researcher in Russia Studies at the Leuven Centre for Global Governance Studies (GGS). Her research is situated within the framework of the project CONNECTIVITY, which focusses on how differences between prominent states' conceptualization of international norms impact upon cooperation in the international system. Her PhD thesis "Defining virtual borders – the impact of securitizing and civilizational narratives on the formation of Internet policy by Russia" focuses on the evolution of Russia's policy on cyberspace governance both domestically and abroad.

Rebecca Mignot-Mahdavi is researcher in international law and counter-terrorism at the T.M.C. Asser Institute and managing editor of the Yearbook of International Humanitarian Law. Previously, she was a PhD candidate at the European University Institute where she will defend her dissertation in December 2020, and a project collaborator with the ERC project 'The Individualization of War'. She previously taught at SciencesPo Paris' Euro-American campus, was a Research Fellow at the Human Rights Institute of Columbia Law School and spent a year at the Institute for Strategic Research (French Ministry of Defense Research Institute).

Stef Wittendorp is lecturer and researcher at Leiden University and a PhD candidate at the University of Groningen. His research interests include counter-terrorism, the regulation of mobility and critical security studies. He is the editor, together with Matthias Leese, of *Security/Mobility: Politics of Movement* (Manchester University Press, 2017).

Contact information

E-mail: info@thehaguecybernorms.nl
Website: https://www.thehaguecybernorms.nl
@HagueCyberNorms

Address
The Hague Program for Cyber Norms
Faculty of Governance and Global Affairs
Leiden University
Hague Campus
Turfmarkt 99
2511 DP The Hague

Colofon
Published October 2020.

Graphic design: www.pauloram.nl

THE HAGUE
PROGRAM
for Cyber Norms

Universiteit
Leiden