Studies in Conflict & Terrorism

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/uter20

Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy

Dennis Broeders, Fabio Cristiano & Daan Weggemans

To cite this article: Dennis Broeders, Fabio Cristiano & Daan Weggemans (2021): Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy, Studies in Conflict & Terrorism, DOI: 10.1080/1057610X.2021.1928887

To link to this article: https://doi.org/10.1080/1057610X.2021.1928887

Published online: 02 Jun 2021.

STUDIES IN CONFLICT & TERRORISM
https://doi.org/10.1080/1057610X.2021.1928887

Routledge
Taylor & Francis Group

Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy

Dennis Broeders, Fabio Cristiano and Daan Weggemans

Institute of Security and Global Affairs, Leiden University, The Hague, The Netherlands

ABSTRACT

This article analyses the evolution and interplay of national policies and international diplomacy on cyber terrorism within and across the UNSC's permanent five members and the UN process on cyber norms (GGE and OEWG). First, it reveals how – through the extension of preemptive measures to low-impact cyber activities and online content – national policies progressively articulate cyber terrorism as an issue of information security. Second, it problematizes how – through the adoption of comprehensive and imprecise definitions – the diplomatic language on cyber terrorism might lend international support to those authoritarian regimes keen on leveraging counter-terrorism to persecute domestic oppositions and vulnerable groups. Third, it concludes that – with UN diplomatic efforts increasingly discussing countering (dis)information operations – combining normative debates on cyber terrorism with those on information security requires precision of language to safeguard human rights globally.

ARTICLE HISTORY
Received 1 April 2021
Accepted 9 May 2021

Cyber terrorism is an elusive concept. Most definitions make a distinction between on the one hand politically motivated violent acts, or the threat thereof, using the internet, and on the other hand all the preparatory and supporting activities for terrorism done on or via the internet, such as recruitment, communication and financing. Governments fear the violent terrorist act the most but, given that "pure" cyber terrorism has not yet materialized, have mostly focused on countering the preparatory and supporting digital activities of suspected terrorists and radicalized actors. Given the "low probability, high impact" character of terrorism, counter terrorism policies have seen a high degree of political and legal exceptionalism, especially in the wake of the 9-11 attacks and the ensuing "war on terror".[1]

Given that cyber terrorism is part and parcel of the digital domain, cyber counter terrorism has become intertwined with another general trend in national security and law enforcement, that of the development of the digital surveillance state.[2] The general trend of states trying to increase security by means of online surveillance has been prevalent in international security and foreign intelligence[3] and in domestic and international law enforcement.[4] This has sparked many debates about the proportionality

CONTACT Dennis Broeders d.w.j.broeders@fgga.leidenuniv.nl Institute of Security and Global Affairs, Leiden University, The Hague, The Netherlands.

and effectiveness of digital surveillance, tensions with and violations of fundamental rights such as privacy and freedom of speech, the unequal treatment of suspects as a result of hard coding bias into surveillance technologies, and tensions with procedural rights such the presumption of innocence due to the increasingly preemptive character of surveillance technologies.[5]

Stretching the reach of digital surveillance powers is facilitated when it is done in support of counter cyber terrorism, a concept that is stretchy in itself. Moreover, authoritarian regimes have been known to use the language of counter terrorism to control and persecute domestic political opposition and national or ethnic minorities.[6] Western states have at times called out such misappropriations of shared language for national security interests as violations of (digital) rights and freedoms.[7] Any normalization of exceptional measures in the name of counter terrorism, which are also present in digital surveillance practices in liberal democracies, weakens the western position as a global normative advocate of (digital) rights worldwide, and may provide a renewed legitimacy to those authoritarian regimes that label domestic actors as terrorists. Framing unwanted cyber activities in discourses of cyber terrorism allows autocratic regimes to build a wider regime of domestic repression, while deflecting international criticism by pointing to similar Western discourses phrased in familiar vocabulary and narratives. In the international domain it is often diplomats that are required to square this circle.

One of the places where the international community discusses the issue of cyber terrorism is the "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security" (hereafter UN GGE). This longer running process is currently paralleled by the work of a newly established UN Open-Ended Working Group (OEWG) for cyberspace, with roughly the same mandate. The first process is championed by the United States and its allies, the second by Russia and China and their allies (see section 4 for more background on these processes)

This article investigates, firstly, the interaction effects between the development of national counter cyber terrorism legislation, with a focus on policy developments in the permanent five of the UN, and the international discussions on cyber terrorism at the level of the UN GGE and OEWG. Secondly, it looks at the interaction effects between the diplomatic language on counter cyber terrorism, fundamental human rights discourse and specific debates in international cyber security that may bear upon the issue of cyber terrorism. Most notably this concerns the emerging problem of information operations and disinformation and the related diplomatic discussion about "cyber security" versus "information security". The first may be seen as a vertical relationship between the national and the international, the second as a horizontal relationship between issues or themes discussed in the same international negotiations – although these are obviously informed by national positions and legislation.

Whereas academic scholarship has primarly engaged with the issue of cyber terrorism in conceptual terms, this article also contributes to the debate through an empirically-sound analysis of national policies and international diplomacy as a way to reveal the political stakes at play with the mainstreaming of the narrative of cyber terrorism. Following this introduction, Section 2 will look at the way conceptions of

cyber terrorism and counter cyber terrorism have developed in academic and policy circles. While academics have defined cyber terrorism often in a narrow sense – referring to violent terrorist attacks via cyberspace – others use the concept to refer to a much broader range of online terrorist activities. Meanwhile, policies have been developed to counter both forms. These policies are characterized by a strong preemptive logic, which, in the case of broader understandings of cyber terrorism, inevitably touches domains such as freedom of speech. Section 3 will look at the evolution of national counter cyber terrorism policies, or more broadly the cyberspace elements of counter terrorism policies, in China, France, the United Kingdom, the United States and Russia.[8] In the name of preemption, and through the extension of exceptional responses to low-risk online activities, these national policies increasingly turn cyber terrorism into an issue of information security, thus also threatening freedom of speech. Section 4 will look into the role that cyber terrorism plays in the UN GGE and OEWG negotiations and which other themes connect to policies of countering terrorism, or anything characterized as such, online. The rise of disinformation campaigns, and the role of the big social media platforms, are putting pressure on western countries to discuss the integrity of information – engaging with the authoritarian discourse on information security – without damaging the human rights framework. Section 5 discusses the interlinkages between national policy development and the international diplomatic debate in the GGE and the OEWG and the interlinkages between different themes in these diplomatic processes that touch on cyber terrorism, digital surveillance, and human rights.

Mapping the Concept: How Cyber and Terrorism Are Stretched in Theory

Cyber terrorism is an essentially contested concept. There exist widely differing views on what constitutes a cyber terrorist act.[9] Let us start with the traditional notion of terrorism here, which can be broadly defined as "premeditated, politically motivated violence – or the threat of violence – against noncombatants or property by subnational groups or clandestine agents to influence, coerce, or intimidate an audience extending beyond the immediate target of the attack".[10] Cyber terrorism, by extension, is where terrorism and cyberspace meet. The term was first coined in the 1980s by Collin and is now widely used by policymakers, politicians, law enforcement, academics and media in rather diverging ways. In academia, cyber terrorism is commonly used to refer to terrorist attacks carried out via cyberspace or "hacking with a body count" to use Collin's turn of phrase.[11] Perhaps the most influential understanding of cyber terrorism is that of Dorothy Denning (2000) who defines it as: "unlawful attacks and threats of attacks against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives".[12] She also highlights that, in order to qualify as cyber terrorism, an attack must have an impact in the "real world" that goes well beyond damage to data or information technologies:

> To qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be

> examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.[13]

Similarly, Pollitt defines cyber terrorism as "the premeditated, politically motivated attack against information computer systems, computer programs, and data which result in violence against noncombatant targets by sub-national groups or clandestine agents"[14] and Hua and Bapna define it as "an activity implemented by computer, network, Internet, and IT intended to interfere with the political, social, or economic functioning of a group, organization, or country; or to induce physical violence or fear; motivated by traditional terrorism ideologies".[15]

Cyber terrorism in this violent sense has never occurred – there is no evidence of terrorists resorting to computers to kill or destructively disrupt societies and most scholars think it is unlikely they will do so any time soon.[16] According to Maura Conway, cyber attacks are vastly expensive, terrorist groups typically lack the skills for successful cyber attacks, the destructive potential of physical attacks can be more readily materialized, and cyber terrorism lacks the theatricality of conventional attacks and is therefore less attractive to terrorist groups.[17] Hence, as Myriam Dunn Cavely summarizes it: "while governments and the media repeatedly distribute information about cyber-threats, real cyber attacks resulting in deaths and injuries remain largely the stuff of Hollywood movies or conspiracy theory. In fact, menacing scenarios of major disruptive occurrences in the cyber-domain, triggered by malicious actors, have remained just that – scenarios".[18]

Some have suggested that this very absence of cyber terrorism indicates that the concept should be redefined and focus more on the different ways terrorist groups utilize cyberspace in support of their agendas. Evan Kohlmann, a terrorism analyst, for example refers to cyber terrorism as "any application of terrorism on the internet".[19] In this approach, cyber terrorism encapsulates a diverse range of online terrorist activities in cyberspace such as communication, recruitment, coordination, fundraising, planning, intelligence gathering, etc.[20] Sarah Gordon and Richard Ford take a similar approach and argue that terrorists targeting computers, networks and the information stored therein can be considered "pure cyber terrorism", while they see "traditional cyber terrorism" when terrorists leverage the "many factors and abilities of the virtual world (.) in order to complete [their] mission".[21]

This broad, nonviolent, approach to cyber terrorism, in which computers can be either the *target* or the *tool* of terrorists, is popular among journalists and the public.[22] Similarly, some policy organizations have also been seduced by broad definitions of cyber terrorism. For instance, the National Conference of State Legislatures, which helps policymakers in the U.S. with pressing issues, has defined cyber terrorism as:

> The use of information technology by terrorist groups and individuals to further their agenda. This can include use of information technology to organize and execute attacks against networks, computer systems and telecommunications infrastructures, or for exchanging information or making threats electronically.[23]

Scholars, on the other hand, remain defensive against such broad labeling as it suggests that cyber terrorism is a pervasive phenomenon or simply because it does

not seem to add much to speak of cyber terrorism as "almost any use of information technology by terrorists".[24] Michael Kennedy, for example, has argued that, just like it makes little sense to refer to terrorists using cell-phones as "cell phone terrorism" we should not speak of terrorists exploiting the Net to facilitate their acts as cyber terrorism.[25] In such broad understandings the connection with the constitutive elements of traditional terrorism, such as politically motivated violence and the incitement of fear has become obscured. This is not to say academics over the last years have not been interested in terrorist's use of cyberspace. On the contrary, the internet is considered by leading scholars as one of the "hot topics"[26] in terrorism research and many interesting articles have been published on terrorist use of the internet.[27] But for most academics the label cyber terrorism remains reserved for terrorism involving computers as weapon *and* target. For them, as Conway concludes, "terrorist 'use' of computers as a facilitator of their activities, whether for propaganda, communication, or other purposes, is simply that: 'use'".[28]

Meanwhile, national strategies have been developed to counter both violent and nonviolent forms of cyber terrorism. In order to understand the underlying mechanisms of comptemporary (cyber) counterterrorism frameworks, the historical and ideological context of the war on terror and its inherent logic of preemptive security must be thus taken into account. In *The Politics of Possibility*, Louise Amoore argues that the mode of governance of post-9/11 security relies on an *anticipatory logic* which "acts not strictly to *prevent* the playing out of a particular course of events on the basis of past data tracked forward into probable futures but to *preempt* an unfolding and emergent event in relation to an array of possible projected futures".[29] This logic is reflected in a shift from probability to possibility in security decision-making, and thus cyber attacks done by terrorists are considered dangerous "not because of what they have (or have not) done to date, but precisely, because they threaten to generate serious impacts in the future".[30] As stated by infosec entrepreneur, and former military, Chad Parks already in 2003:

> It is true that America has never suffered consequences of a true cyber terrorist attack, yet. On September 10, 2001, it was also true that no organized terrorist group had ever hijacked four airplanes, crashed two into the World Trade Center, one into the Pentagon, and one in a field in Pennsylvania, killing over three thousand Americans.[31]

Similarly, policies focusing on the broader terrorist use of cyberspace (e.g. removing online extremist content or shutting down websites) are also legitimized by the aim to intervene "left from the bang" – to preempt terrorist activity or to suppress it if it occurs. Preemption of terrorism on the internet, then, largely entails monitoring and assessing intents by reading meaning into online content. As such, countering these broader manifestations of cyber terrorism constitutes a potential danger for *freedom of speech*. Jack Balkin explains that free speech in an online setting is no longer "dualist", i.e. consisting of a territorial government as the censor and a private individual or group of individuals as the speaker.[32] Rather, free speech online constitutes a "triangle" of speakers: nation-states, internet infrastructure companies and a variety of individual speakers. The shift on content marks a different moment in the relationship between preemption and security as it moves the focus not only from effect to intent, but also got us into the complex domain of semantics (from

the bad guys to the bad content). But, what is "bad" content and who gets to decide it?

National Policies and the Stretching in Practice

Waiting for a Catastrophe: The Pre-Emptive Legacy of the "War on Terror"

In the early 2000s, cyberspace emerged as a prominent milieu of international security and warfare. At the same time, the terrorist attacks on 9-11 brought attention to the possibility of cyber terrorism and lead to the emergence of a host of national policies countering, as well as theorizing, the upcoming catastrophic phenomenon. Early scholarly work on cyber terrorism originated within those American policy circles wherein academic research intersected with, and cross-fertilized, national defense, intelligence, and law enforcement. As shown by Denning's well-known definition sketched during a policy consultation at the U.S. House of Representatives in 2000, national policy debates have been forerunners in theorizing and normalizing the language of cyber terrorism across academic and public narratives. As early as October 1999,[33] the Naval Post Graduate School published "the first and to date most comprehensive study on "cyber terror" for the U.S. Defense Intelligence Agency".[34] The authors marked a clear distinction between "pure" cyber terrorism and other terrorist activities online by stating that the "terrorist use of information technology in their support activities does not qualify as cyber terrorism".[35]

At this point, national policies and law enforcement referred to cyber terrorism as a "possibility", with no substantial indicators pointing at its imminent occurrence. In 2002, when the FBI circulated an advisory note on the possibility of terrorists to recur to cyber attacks, it also specified that "although the FBI possesses no specific threat information regarding these apparent intrusions, these types of activities on the part of terrorists pose serious challenges to our national security".[36] In the same year, the CIA circulated a memorandum indicating that Al Qaida had "far more interest in cyber terrorism than previously believed" and had contemplated "the use of hackers for hire to speed the acquisition of capabilities".[37] As shown by the CIA's document, cyber terrorism entered the national public discourse as an issue of both domestic and international relevance because of its possible *effects*, with the label of terrorist in this specific case being stretched to hackers "for hire".[38]

The fear of a high-consequence threat also justified the stretching of the war on terror's anticipatory logic, and its exceptional security measures, to a broader range of online activities in order to preempt terrorist violent attacks.[39] The *U.S. Patriot Act* 2001 blurred the operational lines between different national security domains – such as defense, intelligence, law enforcement, etc. – and those between domestic and international competencies.[40] By doing so, it widened the set of tools available to law enforcement for preventing and prosecuting cyber terrorism.[41] Spread across different U.S. departments and agencies, counter cyber terrorism did not ultimately institutionalize into a single policy or operational domain.[42]

Over the years, while pure cyber terrorism did not materialize in the forms imagined within the narrative on the war on terror, terrorists marked their presence in cyberspace differently. As early as the end of the 2000s, cyberspace had become "the

most important meeting place for jihadis all over the world, to communicate, discuss, and share their views".[43] In spite of this, national security policies and political discourses continued to normalize the possibility of pure cyber terrorism as the primary point of reference for their counter-terrorism strategies, also through bilateral international cooperation.[44]

In 2011, the United Kingdom's Home Secretary Theresa May argued in a speech given to the Council on Foreign Relations in Washington that "we continue to see little evidence of systematic cyber terrorism. But this is now part of the language of Al Qa'ida. As a tactic, and as a weapon, cyber terrorism is perfectly suited to the world of the lone terrorist, operating outside a hierarchy and without traditional command and control".[45] At a reception hosted for Commonwealth leaders during the United Nations General Assembly six years later, in 2017, the now Prime Minister confirmed that: "we face new and unprecedented joint challenges: (…) how to address new security challenges, like cyber terrorism, and online extremism, and so create a more secure Commonwealth; and how to protect and promote the values we all share and so create a fairer, freer and more tolerant Commonwealth".[46]

National Legislations of the P5: Stretching Cyber Terrorism beyond Its "Pure" Form

National security policies, reinforced by recent terrorist attacks in Europe, have thus contributed to making cyber terrorism one of the most known of the catastrophic unknowns.[47] While this possibility continues to be engrained into national policy narratives, the original distinction between pure cyber terrorism and other terrorist activities online has generally faded away. Most governments address the overall threat of "online terrorism" by employing a mixed policy strategy that combines general criminal laws and counter-terrorism legislations, as well as cyber-crime and cyber security legislative frameworks.[48]

The most recent White House's *National Cyber Strategy (2018)* does not make any reference to cyber terrorism. Rather, Donald Trump's hand-signed national strategy addresses the question of online terrorism only in the section on American international influence: "We will also work to prevent authoritarian states that view the open Internet as a political threat from transforming the free and open Internet into an authoritarian web under their control, under the guise of security or countering terrorism". As a pillar of American influence on cyber issues, it continues: "As such, United States Internet freedom principles are inextricably linked to our national security. Internet freedom is also a key guiding principle with respect to other United States foreign policy issues, such as cybercrime and counterterrorism efforts".[49] This U.S. strategy frames the issue of online terrorism in terms of international cooperation, influence, and as a trope of soft power, rather than one of national security or sovereignty.

Contrarily, the United Kingdom strongly upholds the language of cyber terrorism.[50] The *National Security Strategy* 2015 acknowledges in fact that cyber terrorism constitutes a "significant and varied threat" because "terrorists and cyber criminals can use easily available cyber tools and technology for destructive purposes".[51] Further advancing

this policy perspective, the *National Cyber Security Strategy* 2016–2021 confirms that "terrorist groups continue to aspire to conduct damaging cyber activity against the U.K. and its interests", while assessing their current technical capabilities as low.[52]

Interestingly, the document argues that "the impact of even low-capability activity against the U.K. to date has been disproportionately high: simple defacements and doxing activity (where hacked personal details are 'leaked' online) enable terrorist groups and their supporters to attract media attention and intimidate their victims".[53] By doing so, the policy document makes an explicit reference to the "high impact" obtainable through low intensity disruptions in terms of publicity: "the technical capability of terrorists currently remains limited but they continue to aspire to conduct damaging computer network operations against the U.K., with publicity and disruption as the primary objective of their cyber activity".[54] Additionally, as "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 U.K. and its interests".[55] In line with the country's growing strategic interest in offensive cyber capabilities, the document envisions the possibility of recurring to hardcore preemptive measures "through the identification and disruption of terrorist cyber actors who currently hold, and aspire to build, capability that could threaten U.K. national security".[56] The document in fact leverages on the threat of cyber terrorism in order to outline the country's National Offensive Cyber Program (NOCP) as an element of "*Enhancing Sovereign Capabilities – Offensive Cyber*": "offensive cyber forms are part of the full spectrum of capabilities we will develop to deter adversaries and to deny them opportunities to attack us, in both cyberspace and the physical sphere".[57]

France upholds an identical position on the matter. In the 2019's Ministry of Defense's *Eléments publics de doctrine militaire de lutte informatique offensive,* the "risk of terrorism" is mentioned as one of the elements making the adoption of a cyber-offensive strategy necessary.[58] The French *National Digital Security Strategy* 2015 echoes the U.K.'s stance by arguing that the intensity of terrorists' cyber attacks shall not be measured in terms of actual damages, but in relation to their "high symbolic value": "in parallel, the positions taken by France on the international scene, its military operations and certain public debates are followed by cyber attacks aimed at marking public opinion. For example, the defacement of many websites after the terrorist attacks that targeted France in the beginning of 2015 had a technically low but symbolically high impact desired by the attackers".[59]

Elsewhere, where counter cyber terrorism policies developed outside the direct legacy of the war on terror, national policies on cyber terrorism trace a less clear demarcation between the different types of terrorist activities online. In China, national policies do not mark a distinction between online and offline terrorism, nor do they differentiate between "pure" activities and incitement, planning, fundraising, etc.[60] Different legislations – *Criminal Law* 2015,[61] *Counterterrorism Law* 2016[62] and *Cybersecurity Law* 2017[63] – regard the internet as a medium or tool through which a criminal act may be committed, rather than an independent constituent element of the crime. In light of foundational Chinese policy concepts such as information security and digital sovereignty, focused on control on information and regime continuity, cyber terrorism is best understood to refer to a number of online activities deemed to meet

the very broad criteria that define "terrorism" and "terrorist acts" set out in other legislations, rather than in relation to its pure or not pure elements.[64]

According to Art. 3 of the *Counterterrorism Law*, terrorism broadly refers to any action taken to "create social panic, endanger public safety, violate persons or property, or coerce national organs or international organizations". The Counterterrorism Law gives expansive and blurring definitions of "terrorism" and "extremism", with "fake terrorism information" presented as one of the tools available to extremists' propaganda. This was first explicitly addressed in Art. 120(b) of the ninth amendment to the *Criminal Law* in 2015, which stipulated a minimum of a five-year criminal sentence for 'advocating terrorism or extremism through methods such as using audio-visual materials and information networks. Promulged two years later, Art. 12 of the *Cybersecurity Law* similarly exhorts that "any person or organization using a network must not use the network to propagate terrorism or extremism".[65] Through different complementing regulations, cyber-terrorism as a concept has been wholly integrated, albeit implicitly, into the broader agenda of the Chinese Party-state to fully regulate, securitize, and surveil its sovereign cyberspace.[66] Interestingly, China has however specifically addressed the issue of cyber terrorism in more explicit terms in its recent contribution to the OEWG (see section four).

The Russian federation has taken a different approach to the issue of cyber terrorism in its recent legislations by clearly endorsing the possibility of pure cyber terrorism in its legislative frameworks as a threat to information security. Russian national cyber security strategies have, over the years, addressed the threat of pure cyber terrorism in relation to the protection of the country's critical infrastructures.[67] For example, the *Strategy for National Security* 2015 enlists cyber disruptions as one of the main aims of the activities of terrorist and extremist organizations.[68] Further delineating cyber terrorism as an issue of information security, the *Doctrine for Information Security* 2016–2017 warns against the risk of possible disruptions caused by "terrorist and extremist organizations" through the creation of "means to have a destructive impact on critical information infrastructure for unlawful purposes".[69] According to this policy, terrorist activities listed as basic information threats include "mechanisms of information influencing", the incitement of ethnic and religious hate, the promotion of extremist ideologies, and recruitment. The Russian doctrine of information security does not in fact mark a distinction between the physical-infrastructural element of the "infosphere" (and not cyberspace) from its contents: "the Doctrine defines the information sphere as a combination of information, informatization objects, information systems and websites within the information and telecommunications network of the Internet, communications networks, information technologies, entities involved in generating and processing information, developing and using the above technologies, and ensuring information security, as well as a set of mechanisms regulating public relations in the sphere".[70]

Threatening Freedom of Speech: From "Bad" Guys to "Bad" Content

Using increasingly broad definitions of cyber terrorism, the P5 are shifting – to different extents – the focus of their counter strategies from possible "*effects*" to relevant

"*intents*".[71] This means that national security policies now aim to regulate the dissemination of terrorist content not only in relation to possible violent acts (online and offline), but also to incitement, support, and glorification. Through the extension of the logic of preemption to speech, these goverments require more sophisticated surveillance techniques – such as automated content moderation and censorship, predictive policing, and more.[72] In so far as the responsibility for contents ultimately remains with the "hosts", this "war on words" has further diluted agency and sovereignty by including actors other than the state into the execution of national security policies: social media platforms, surveillance technologies, automated algorithms, etc.[73] While Western countries have traditionally stayed away from online content moderation on social media platforms, the growing speed and rise in "bad" content – beyond terrorism – has marked a clear shift: they are increasingly stepping up and/or require social media platforms and "tech giants" to step up.[74]

Above all, the so-called "war on words" pertains to the access, moderation, and censorship of "bad" content online. The United Kingdom's *Counter Terrorism and Border Security Act* 2019 goes much further than previous acts in policing behaviors that can be considered to be removed from both terrorist violent effects or even intent. It criminalizes, for instance, the one-time viewing of information online that authorities consider planning a terrorist attack. Parliament's Joint Committee on Human Rights warned in 2018, that this could easily criminalize "inquisitive or foolish minds".[75] Similarly, expressing support for a terrorist organization, while aware of a risk of encouraging others to do so, also constitutes a crime, and can be punished with up to ten years in prison. As further specified in the U.K. Home Office's *Online Harms White Paper*, the government puts "high expectations" on "companies to go much further and demonstrate the steps taken to combat the dissemination of associated content and illegal behaviors".[76] Several critical responses have emerged in the U.K. pointing at the risks associated to multi-stakeholder/PPP models of content moderation: normative vagueness can in fact outsource excessive discretionary powers to private companies, eroding sovereign prerogatives.[77]

A similar, and perhaps the most decisive, approach to online content moderation has been taken by the French government in the wake of the recent terrorist attacks.[78] Envisioning a strong partnership with major internet companies and social media platforms France, under the presidency of Emmanuel Macron, has positioned itself as leading normative power on collaborative content moderation. The Élysée has been the driving force behind the proposal for the *EU terrorist content regulation* in 2018 for preventing the dissemination of illegal and harmful terrorist content online.[79] The regulation, referred to as TERREG, has been met from the very beginning, with hasrh criticism: a global coalition of NGOs, media groups, and two UN Special Rapporteurs raised strong objections and proposed amendments to the initial draft document for the threat it poses to freedom of speech.[80] After several postponements over the last years, the European Parliament finally approved the TERREG on 28 April 2021, mostly confirming the legislation's initial, and contested, objectices.[81]

As the work on terrorist content regulation has been proceeding at a slow pace at the EU level,[82] the French government went ahead with its national adoption of the regulation.[83] On 19 June 2020, however, France's Constitutional Court turned down

the legislation for being unconstitutional on the grounds of its infringement of "freedom of expression" in a manner that is not "necessary or proportionate" to the law's purpose.[84] The French government has also championed international cooperation between governments and relevant tech companies to fight terrorist content online. In the aftermath of March 2019s terrorist attacks in New Zealand, that were live and broadcasted in full by the perpetrators on Facebook, Emmanuel Macron and New Zealand's Prime Minister Jacinda Ardern met top executives from Google, Facebook, and Twitter to launch and endorse the so-called *Christchurch Call*.[85] With the aim to promote a "free, open, and secure" internet – and based on the belief that platforms are "the publisher, not just the postman" (as eloquently put by Jacinda Ardern) – the call recognized that "the dissemination of such content online has adverse impacts on the human rights of the victims, on our collective security and on people all over the world". While receiving broad international support, from both states and tech companies,[86] France and the United Kingdom have been the only endorsers amongst the P5.[87] In light of an overall less collaborative approach with social media platforms and tech companies, and with a strong normative tradition safeguarding freedom of speech, the United States did not in fact sign the Christchurch Call. In a note, the White House praised the initiative but also stated that was "not currently in a position to join the endorsement". Coherently with its national cyber strategy, the White House stated that "we encourage technology companies to enforce their terms of service and community standards that forbid the use of their platforms for terrorist purposes", and that "we maintain that the best tool to defeat terrorist speech is productive speech and thus we emphasize the importance of promoting credible, alternative narratives as the primary means by which we can defeat terrorist messaging".[88] In a commentary on the Christchurch Call, the Russian International Affairs Council (RIAC), a think tank founded by presidential decree, saluted the development claiming Russian and Chinese "ownership" for its strategy:

> One of the most recent trends to appear in internet governance is the tightening of control over online content. And it was China and Russia that set the wheels for this in motion.[89]

This is not far from the truth. Through the *Sovereign Internet Law* 2019, Russian authorities justified wider monitoring of social media and the prohibition of the use of anonymizers and VPNs to access website containing forbidden content. Rather than outsourcing responsibility to foreign tech companies – defined in the legislation as "information dissemination organizers" – Russian authorities have required internet service providers (ISPs) to install software allowing authorities themselves to access (and to block) online contents. These provisions further expand the surveillance powers contained in the so-called *Yarovaya Counterterrorism Law* 2018, such as the requirement for content hosts to store and share information about users with national security authorities without a court order. Human Rights Watch has strongly criticized such legislations because they "enable the government to directly block whatever content it deems undesirable".[90]

Chinese authorities showed, through the *National Cyberspace Security Strategy* 2017, a similar concern in 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",[91] meanwhile "operating one of the most sophisticated systems for online censorship and surveillance of its own citizens".[92] As argued by Human Rights Watch, "China's terrorism prosecutions, primarily in the northwestern region of Xinjiang, are subject to politically motivated abuse because of the expansive definition of terrorism, lack of transparency, and violations of fair trial rights". At the same time, little evidence exists as "failure to release details about terrorism convictions heightens concerns that the country's counterterrorism law is being used to prosecute nonviolent activity".[93] The 2016 Supreme People's Court (SPC) annual report – the latest resource containing specific figures on terrorism prosecutions and convictions – stated that in 2015, Chinese courts convicted 1,419 people for threatening state security, inciting "splittism" and "terrorism". Of these, only four court verdicts are publicly available and indicated that, all but one of the seven involved people were ethnic Uyghurs from Xinjiang convicted for: possessing, accessing, and distributing terrorism-related videos or audios: clicking on weblinks that contained images of flags of the East Turkestan Islamic Movement (ETIM), or videos about Rebiya Kadeer, leader of exiled Uyghurs.[94]

Summing up, the analysis of these policies indicates that while the possibility of cyber terrorism still permeates the national security agendas of the UNSC's permanent members, counterterrorism and preemptive responses have now been extended beyond high-impact activities. National policies increasingly focus on online content and, by doing so, articulate cyber/online terrorism as an issue of information security. As shown in this section's analysis, this has important consequences at the national level for human rights in general, and for freedom of speech in particular. An important ensuing question is how these debates are reflected in the international diplomacy on cyber norms?

Interaction Effects between the National and the International

Even though pure cyber terrorism has not yet happened – states are still preoccupied with the possibility. Within the UN ecosystem there are different bodies that address (cyber)terrorism, most notably the UN Security Council, the third committee that deals, amongst other things, with crime prevention and criminal justice, and the first committee that deals with disarmament and international security.[95] Security related aspects of ICTs or the cyber domain, have been discussed foremost in the "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security" (hereafter UN GGE). This process started in 2004, is currently in its sixth iteration, and is one of the main fora where diplomats discuss the issue of cyber terrorism. The GGEs take place within the first committee of the UN and are therefore rooted in the domain of disarmament and international security, rather than crime and law enforcement. As such, cyber terrorism is not the core interest of these UN "negotiations", but it is one of the few diplomatic fora where the concept is discussed.

As diplomacy plays a vital role in the construction of the international language used to address problems of cyber terrorism and online radicalization, it is important to see how the issue is discussed in the context of the UN GGE. As the UN GGE is a closed doors process we only get to see its end product – a consensus report – if

the group is able to reach consensus, as it only did in 2010, 2013 and 2015.[96] However, at the time of writing (2020) there are two, parallel processes on international security and cyberspace running under the auspices of the UN first committee.[97] In November 2018 the UN General Assembly adopted two resolutions: one American-backed resolution calling for a sixth UN GGE (2019–2021)[98] and a Russian- backed initiative establishing the first UN Open-Ended Working Group (OEWG) for cyberspace.[99] The mandates of these two processes overlap for 90 percent, but the membership is vastly different. The UN GGE consists of 25 national experts negotiating a report, while the OEWG is open to all UN member states. Importantly, the OEWG deliberates in public and states are able to submit their viewpoints on paper to the working group and the public at large. Many do so, and their submissions give insight into the various positions taken and how they develop during the negotiations.[100]

UN GGE 2004–2021

The point of departure for the UN GGE is very different for the main "camps" in the international debate. Russia initiated the UN debate about ICTs in 1998 – calling for the negotiation of a special treaty for cyberspace[101] – because it feared the internet as a vehicle for information weapons. At the domestic level Russia feared free and unfettered access to, and circulation of, information. Internationally, it feared foreign information operations and its effects on regime stability.[102] China took a similar position.[103] Western countries, in this debate loosely assembled under the umbrella of the "like-minded" states, started out from a position that championed the cause of an "open, free and secure internet". The internet was seen as a positive phenomenon, spurring economic growth and spreading the benefits of global access to information and free speech. In many likeminded countries foreign policy related to the internet started out as agendas of "internet freedom", like the one that was spearheaded by Hillary Clinton during her term as U.S. Foreign Secretary.[104] In these initial policies, (digital) human rights were at the forefront of foreign policy and they also guided much of the work done within the UN system by special UN bodies and rapporteurs.[105] However, as the internet became more central to national economies and societies and the (perceived) threats to national and international security grew, foreign policy for the internet became much more firmly embedded in a security perspective.[106] In parallel, the (perceived) threat of terrorism grew, through terrorist attacks all over the globe, the rise of territorial terrorist enclaves in Iraq and Syria and the use of modern ICTs and the internet to promote, finance and further terrorist causes.[107] These shifts have also influenced diplomatic negotiations on ICTs and international peace and security, including how cyber terrorism has been addressed in the UN GGE.

In the cumulative UN GGE consensus reports cyber terrorism gets an ever more important place in the text.[108] In 2010 cyber terrorism made its first appearance in the threat section of the first GGE consensus report:

> Thus far, there are few indications of terrorist attempts to compromise or disable ICT infrastructure or to execute operations using ICTs, although they may intensify in the future. At the present time terrorists mostly rely on these technologies to communicate,

> collect information, recruit, organize, promote their ideas and actions, and solicit funding, but could eventually adopt the use of ICTs for attack.[109]

The combination of there being no cases or even "few indications of terrorist attempts" to use the internet in a damaging way carries on into the reports that follow. Another common thread is the fact that the UN GGE reports set terrorist use of the internet for communication, funding and recruitment etc. apart from the violent terrorist use of the internet, but include both in the text. The latter may be the bigger worry, but the former gets more attention as it pertains to actual ongoing problems. The 2013 report underscores that terrorist groups use ICTs to communicate, recruit, organize and finance, and then moves on to the bigger (if still hypothetical) threat: "If such groups acquire attack tools, they could carry out disruptive ICT activities".[110] Other sections of the 2013 report underscore the need for international cooperation and "bilateral, regional, multilateral and international capacity-building efforts" to combat the use of ICTs for criminal and terrorist purposes.[111] The 2015 report again takes the language up a notch, though still only as a possibility, by linking it explicitly to international peace and security, which is the raison d'être of the first committee:

> The use of ICTs for terrorist purposes, beyond recruitment, financing, training and incitement, including for terrorist attacks against ICTs or ICT-dependent infrastructure, is an increasing possibility that, if left unaddressed, may threaten international peace and security.[112]

Further recommendations in the 2015 report call for international cooperation, "in a manner consistent with national and international law"[113] and capacity building efforts.[114] The conclusion of the report furthermore states that "the United Nations should play a leading role in promoting dialogue on the security of ICTs (…) although these efforts should not duplicate ongoing work by other international organizations and forums addressing issues such as criminal and terrorist use of ICTs, human rights and Internet governance".[115] As the 2016–2017 round of the UN GGE failed to produce a consensus report we have no access to the language on cyber terrorism in the draft report, but given the prevalence of terrorist attacks in that period and national legislation addressing terrorism and the use of ICTs, it is safe to say the topic would have been addressed.

Open Ended Working Group 2019–2021

The OEWG is a more transparent process than the UN GGE: its deliberations are public and many states submit their viewpoints on a dedicated UN website.[116] The OEWG wrapped up its work in March 2021, producing the first consensus report on international cyber security whose negotiations were open to all UN member states.[117] During the course of the negotiations the Chair of the OEWG submitted a number of pre-drafts of the report for the UN member states to comment on. Many member states have done so. The initial pre-draft report contains three references to cyber terrorism. Both in the introduction and in the section on establishing a "regular institutional dialogue about cyberspace and international security" it is noted that "discussions on other aspects of digital technologies have advanced in various UN bodies

and agencies" (…) including on "cybercrime and the use of the Internet for terrorist purposes".[118] In the threat section it is noted that "(…) some ICT capabilities previously only available to States were now accessible to non-State actors, including terrorists and criminals", which is by now a familiar phrasing. Most western states either do not mention cyber terrorism in their comments on the draft report or play it down. China and Russia in their turn, use the language on addressing each issue in the right UN forum to argue that references to human rights that "fall within the competence of other UN bodies, look especially inappropriate" in the pre-draft report.[119]

China expresses its concern that the "constructive proposals on issues such as (…) the fight against cyber terrorism" it made during the previous two sessions have not found their way into the text and hopes that these proposals could be incorporated in the report.[120] In an earlier contribution to the OEWG and the UN GGE, China flagged cyber terrorism as a severe threat and proposed a whole section on counter cyber terrorism under the norms section of the report.[121] In addition to states blocking terrorist use of the internet, China specifically calls for "intelligence exchanges and law-enforcement cooperation on countering terrorism" between states, the development of "cooperative partnership with international organizations, enterprises and citizens in fighting cyber terrorism" and states requesting "Internet service providers to cut off the online dissemination channel of terrorist content by closing propaganda websites and accounts and deleting terrorist and violent extremist content". The language of the Chinese contribution is far reaching, could easily be at odds with online freedoms such as freedom of information and expression, and explicitly asks for intermediary censorship content by "enterprises" and "internet service providers".[122]

As some of the Chinese solutions do not differ so much from Western policy proposals – which are also turning to intermediaries, such as social media companies and ISPs, to take down content[123] – the important question comes down to the national definitions and interpretations of cyber terrorism that authorities will employ. Authoritarian governments have been known to stretch the meaning of terrorism and the digital domain will not be an exception. If anything, given the massive investment of authoritarian regimes in surveillance technologies, the digital domain provides an optimal operational ground for a modern police state. Australia's reaction to the Chinese proposals has been to suggest that issues such as counter-terrorism are "better addressed in other forums"[124] but a number of other countries have latched onto the combination of counter terrorism and corporate responsibility, especially when it comes to the role of (Western) social media corporations. For example, the Venezuelan reaction to the initial draft states:

> Venezuela considers that this document should include a reference to the role of digital platforms, companies and States in assuring a responsible behavior that could prevent actions and/or attacks against the territories and critical infrastructure of other States, with a view to avoid the misuse of ICT's for hostile propaganda; interference in the internal affairs of States; violating the national sovereignty, security, public order and health systems of States; discriminatory treatment of information contents and/or disinformation; misuse for criminal and terrorist purposes.[125]

Zimbabwe[126], Iran[127] and the Nonaligned Movement[128] have made similar statements in their reaction to the draft report. Just as some western governments are at least

marginally sympathetic to the need for content moderation by large social media companies – if only out of necessity – the current age of fake news, disinformation, information operations and election interference also brings them much closer to the realm of content moderation and information control than they are comfortable with. The risk of justifying the repression of fundamental rights in authoritarian-ruled countries by providing diplomatic language on the dangers of cyber terrorism, whose meaning can be stretched to include the persecution of regime critics at the domestic level, have made Western countries wary of engaging too much with the debate. Alternatively, they try to embed the issue in the language of human rights protection. Moreover, in the debate about international cyber security specifically, the like-minded have always resisted the Russian and Chinese framing of the diplomatic debate in terms of "information security" and steered the discussion in the direction of "cyber security". The choice for cyber security, with a focus on technical security and the security of vital infrastructures, was in answer to "(…) growing concerns that the broad definition of "information security" advanced by Moscow and Beijing is a Trojan horse for content control and a human rights issues at heart".[129]

Now that western countries are feeling the pinch of information operations and are targeted by foreign efforts to disturb their national information sphere – through information operations that influence and contaminate political and societal debate and in some cases even seek to interfere with elections – they need to find the language to address these issues without getting trapped in the language of "information security".[130] This is new and unfamiliar territory for western diplomats as it puts content and content control center stage, similar to the way cyber terrorism has become enmeshed with content control. France for example, mentions in its reaction to the OEWG draft report that "the issue of interference and disinformation operations (…) while not directly linked to the group's mandate, is a particularly concerning threat".[131] The Dutch position perhaps highlights the double challenge best. The Netherlands clearly condemn the use of "cyber enabled information operations" in the context of healthcare and the COVID-19 crisis as a violation of International law. On the other hand, the Dutch delegation sees the risk for human rights in addressing the issue of disinformation. They therefore advise against deliberating on issues such as "disinformation" in the work of this working group, but should the chair decide otherwise:

> The Netherlands strongly suggests that the report of the OEWG stresses that all countries should ensure that measures to counter "disinformation" are formulated in a way that respects international human rights law and complies with the principles of legality, legitimacy, proportionality and necessity.[132]

The circle that needs to be squared on the issue of information security to a certain degree overlaps with the circle that needs to be squared for cyber terrorism. In both cases western countries (begin to) see the need to address a real and/or potential problem while they are resisting the language used by adversarial states to address the issue. At the same time, they are trying to uphold the language of human rights protection to hold authoritarian states to account when they overstep the boundaries of counter cyber terrorism and information security in western eyes.

The final substantive report of the OEWG that was adopted by consensus in March 2021 does not include any substantial references to cyber terrorism, other than the

familiar notification in the threats section that: "The continuing increase in incidents involving the malicious use of ICTs by State and non-State actors, including terrorists and criminal groups, is a disturbing trend. Some non-State actors have demonstrated ICT capabilities previously only available to States".[133] To some extent this may be the result of the chair's strategy to push all the content that was unlikely to gain consensus – in some versions of the report marked as "discussion sections" – out of the report and into a non-binding, non-consenus "Chair's Summary".[134] Many of the issues raised above have found a place in this document which – as indicated in the OEWG consensus report – is going to be one of the main input documents for new rounds of UN cyber diplomacy, such as the new OEWG 2021–2025 which has already been approved by the UN General Assembly.[135] Given the strong feelings of states on some of these matters – especially when held by powerful states such as China – the issue is certain to resurface.

Discussion and Conclusion

Given the nature of national and international policy processes, the interaction between these levels can at best be argued in terms of plausibility and "guilt by association". There is often no way to substantiate any causal relationships between the development of national policies and international negotiations, although sometimes explicit references are made. The interaction may also be "veiled", especially when states want to (mis)appropriate diplomatic language to deflect attention from, or scrutiny of, national laws and practices. Taking into account these limitations, a number of relevant developments can be highlighted.

While academics have feared that the term cyber terrorism would distract attention from other forms of terrorist use of the internet, policymakers and media have approached the issue with a much broader focus. The policies that developed often focus on both "pure" cyber terrorism and terrorist use of the internet in the broader sense. The interconnection between counter terrorism and surveillance technologies used for law enforcement and international security, pushes counter cyber terrorism policy in the direction of preemption. Consequently, counter cyber terrorism develops with a focus on online behavior related to preparatory and supporting activities for cyber terrorism in terms of probabilities. The combination of surveillance technologies and policies operating on a broader understanding of cyber terrorism, inevitably touches human rights, such as the freedom of speech.

Given the reality of terrorism, and the possibility of cyber terrorism, states have started addressing cyber terrorism – albeit not always explicitly under that name – at both the national and the international level. In the interplay between national and international policymaking, fundamental rights, such as freedom of speech and association, are at risk because liberal democratic states enact policies that push against the boundaries of the protection of fundamental rights, while autocratic regimes in practice aim to push beyond them. However, both do so in reference to a common or similar language centered on countering cyber terrorism. Even though liberal democracies are always at pains to highlight that counter terrorism policies should always be embedded in a human rights framework, the shared language often feels too close

for comfort. At the international level, in formal negotiations, this dynamic intensifies. The language of cyber terrorism always carried a risk of undermining the western support for digital rights online, but does so especially in the context of the first committee of the UN, where the UN GGE and the OEWG negotiations take place. The first committee is centered on international (military) security and by extension the negotiations on responsible rules of state behavior in cyberspace are focused on military, strategic state behavior and the stability of cyberspace. As (cyber) terrorism is not at the center of the deliberations it risks becoming a side issue, or even a bargaining chip in the negotiations. In the state contributions to the OEWG we can see western states downplaying cyber terrorism, but so far language on cyber terrorism has always been included in the UN GGE consensus reports and some countries, like China, are actively pushing the issue.

Some digital rights, such as freedom of speech and information, that are at risk from counter cyber terrorism policies, are also at risk from the problem of countering disinformation and information operations that are currently emerging as a pressing issue in the context of the UN GGE and OEWG. The need to address this issue in the context of the first committee runs the risk of drawing western states into the frame of "information security", and cyber sovereignty. This has been the preferred language of authoritarian states, championed by Russia and China especially, to address the strategic risks of cyberspace, which they place at the level of the national "infosphere". It also brings the roles and responsibilities of big tech and social media platforms and intermediate content regulation and moderation into play. The frame of information security – which has been consistently rejected by western state so far – explicitly opens the door to the issue of regulating content, with potentially damaging consequences for online freedoms. Edging toward a common language on these issues may turn out to be too close for comfort again. One may even speculate whether there is a trade off in diplomatic terms for authoritarian governments. Cyber terrorism has been a useful vehicle to dress up national policies to counter digital political opposition and separatism in a common language. The language of information security – at least in the Russian and Chinese playbook – would encompass all of these. To engage liberal democracies on the terms of information security – effectively legitimizing the language – would be hailed as a big win.

In the context of dealing with cyber terrorism, western governments and scholars need to think about the precision of language – how do they want to deal with the wider category of cyber terrorism that is more content related. While states cannot ignore such terrorist use of the internet as it might foster radicalization and manifestations of terrorism in the "real-world", it is important to be aware of the tension this focus brings with it – such as in relation to the freedom of speech. To be more specific, if wide categories are included in counter cyber terrorism policies, these countries firstly, need to make sure fundamental rights are respected – especially given the fact that terrorism and exceptionalism are almost twinned concepts. This needs to be anchored in national legislation, also in order to be able to argue the case at the international level. Secondly, as "vagueness" in terminology is the ideal avenue to misappropriate counter cyber terrorism policies by authoritarian regimes, precision needs to be the first line of defense.[136] Thirdly, liberal democracies need to find their

own language to engage with countries that favor an approach focused on information security. To do so, they will need to connect information security with values and principles that are constitutive of democracy and freedom as a counter balance to instrumental use of the terminology by authoritarian states. On the topic of election interference for example – a specific and targeted form of information operations aimed at the heart of the democratic process – some scholars have suggested to address these in terms of violations of the principles of nonintervention and national self-determination.[137] Information operations in a wider sense will require more thought by scholars and policymakers to fold the problem into democratic values and principles, but this will need to happen as information operations are both unlikely to disappear from the international debate as well as likely to get entangled further into the debate about cyber terrorism.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes

1. Harold H. Koh, "On American Exceptionalism," *Stanford Law Review* 55, no. 5 (2003): 1479–527; Donald E. Pease, *The New American Exceptionalism* (Minneapolis: University of Minnesota Press, 2009); Andrew W. Neal, *Exceptionalism and the Politics of Counter-Terrorism: Liberty, Security and the War on Terror* (Abingdon: Routledge, 2009).
2. David Lyon, *Surveillance after September 11* (London: Polity Press, 2003); Louise Amoore and Marieke De Goede, "Governance, Risk and Dataveillance in the War on Terror," *Crime, Law and Social Change* 43, no. 2–3 (2005): 149–73; Louise Amoore, "Algorithmic War: Everyday Geographies of the War on Terror," *Antipode* 41 (2008): 49–69.
3. Glen Greenwald, *No place to hide. Edward Snowden, The NSA, and the US Surveillance State* (New York: Metropolitan Books, 2014); Zygmunt Bauman et al., "After Snowden: Rethinking the Impact of Surveillance", *International Political Sociology* 8, no. 2 (2014): 121–144; Ben Buchanan, *The Hacker and the State. Cyber Attacks and the New Normal of Geopolitics* (Cambridge, MA: Harvard University Press: 2020): chapter 1.
4. Dennis Broeders et al., "Big Data and Security Policies: Towards a Framework for Regulating the Phases of Analytics and Use of Big Data," *Computer Law & Security Review* 33, no. 3 (2017): 309–23; Andrew G. Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* (New York: New York University Press, 2017); Didier Bigo, "Digital Surveillance and Everyday Democracy," in *The Routledge International Handbook of Criminology and Human Rights*, ed. Leanne Weber, Elaine Fishwick, and Marinella Marmo (Abingdon: Routledge, 2016): 496–510; Sergei Boeke and Quirine Eijkman, "State Surveillance in Cyberspace: A New Perspective on Digital Data Practices by Intelligence and Security Services," in *Terrorism Online: Politics, Law and Technology*, ed. Lee Jarvis, Stuart MacDonald, and Thomas M. Chen (London: Routledge, 2015): 137–55; Quirine Eijkman and Daan Weggemans, "Open Source Intelligence and Privacy Dilemmas: Is It Time to Reassess State Accountability?," *Security and Human Rights* 23, no. 4 (2013): 285–96.
5. cfr. Clive Walker, "The War of Words with Terrorism: An Assessment of Three Approaches to Pursue and Prevent," *Journal of Conflict and Security Law* 22, no. 3 (2017): 523–51; Marek Palasinski and Lorraine Bowman-Grieve, "Tackling Cyber-Terrorism: Balancing Surveillance with Counter-Communication," *Security Journal* 30, no. 2 (2017): 556–68; and Clive Walker and Ummi Hani Binti Masood, "Domestic Law Responses to Transnational

Cyber attacks and Other Online Harms: Internet Dreams Turned on Internet Nightmares and Back Again," *Notre Dame J. Int'l Comp. L.* 10, no. 1 (2020).

6. Chien-peng Chung, "China's 'War on Terror': September 11 and Uighur Separatism," *Foreign Affairs* 81, no. 4 (2002): 8–12; Pavel K. Baev, "Instrumentalizing Counterterrorism for Regime Consolidation in Putin's Russia," *Studies in Conflict & Terrorism* 27, no. 4 (2004): 337–52; Pavel K. Baev, "Turning Counter-Terrorism into Counter-Revolution: Russia Focuses on Kazakhstan and Engages Turkmenistan," *European Security* 15, no. 1 (2006): 3–22.
7. Fabio Cristiano, Dennis Broeders, and Daan Weggemans, *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, 2020). ISBN: 9789083109596.
8. The empirical focus of this article is primarily on the permanent five members (P5) of the United Nations Security Council because these can be considered normative actors on the issue of cyber terrorism: they have all been targeted by terrorism (at the very least according to their own definition); they have always been part of the UN GGE and OEWG processes and, including the main actors from across the traditional divide (western liberal democracies and authoritarian states), constitute a varied selection of cases.
9. Stefano Armenia and Georgios Tsaples, "Individual Behavior as a Defense in the "War on Cyberterror": A System Dynamics Approach", *Studies in Conflict & Terrorism* 41, no. 2 (2018): 109–32.
10. Jerrold M. Post, Keven G. Ruby and Eric D. Shaw, "From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism," *Terrorism and Political Violence* 12, no. 2 (2000): 100.
11. Cited from: James D. Ballard, Joseph G. Hornik, and Douglas McKenzie, "Technological Facilitation of Terrorism: Definitional, Legal, and Policy Issues," *American Behavioral Scientist* 45, no. 6 (2002): 992.
12. Dorothy E. Denning, "Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services US House of Representatives," *Focus on Terrorism* 9 (2000): 71–76.
13. Ibid.
14. Mark M. Pollitt, "Cyberterrorism—Fact or Fancy?," *Computer Fraud & Security* 2 (1998): 8–10.
15. Jian Hua and Sanjay Bapna, "The Economic Impact of Cyber Terrorism," *The Journal of Strategic Information Systems* 22, no. 2 (2013): 175–86.
16. Maura Conway, "Reality Check: Assessing the (Un) Likelihood of Cyberterrorism," *Cyberterrorism: Understanding, Assessment, and Response*, ed. Thomas M. Chen, Lee Jarvis, and Stuart Macdonald (New York: Springer, 2014), 103–121; Lee Jarvis and Stuart Macdonald, "What Is Cyberterrorism? Findings from a Survey of Researchers," *Terrorism and Political Violence* 27, no. 4 (2015): 657–78; Jian Hua and Sanjay Bapna, "Economic Impact"; Armenia and Tsaples, "Individual behavior".
17. Maura Conway, "Reality check", 103.
18. Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (Abingdon: Routledge, 2007), 3; on scenarios, pre-emption, and cyberwar games, see also Fabio Cristiano, "From Simulations to Simulacra of War: From Simulations to Simulacra of War: Game Scenarios in Cyberwar Exercises," *Journal of War & Culture Studies* 11, no. 1 (2018): 22–37.
19. As cited by Eben Kaplan, "Q&A: Terrorists and the Internet," *Council on Foreign Relations* (6 March 2006), https://archive.nytimes.com/www.nytimes.com/cfr/international/slot2_030606.html (accessed May 19, 2021).
20. See also Lee Jarvis and Stuart Macdonald, "What Is Cyberterrorism? Findings from a Survey of Researchers," *Terrorism and Political Violence* 27, no. 4 (2015): 659.
21. Sarah Gordon and Richard Ford, "Cyberterrorism?," *Computers & Security* 21, no. 7 (2002): 637.

22. Maura Conway, "Cyberterrorism: Hype and Reality," in *Information Warfare: Separating Hype from Reality*, ed. Leigh Armistead (Dulles, VA: Potomac, 2007), 73–93.
23. Cfr. Gary LaFree and Joshua D. Freilich (eds.), *The Handbook of the Criminology of Terrorism* (Chichester: John Wiley & Sons, Inc., 2016), 554.
24. Phillip W. Brunst, "Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet," in *A War on Terror?: The European Stance on a New Threat, Changing Laws and Human Rights Implications*, eds. Marianne Wade and Almir Maljević (New York, NY: Springer, 2010), 51.
25. Michael Kenney, "Cyber-Terrorism in a Post-Stuxnet World," *Orbis* 59, no. 1 (2015): 111–28.
26. Bart Schuurman, "Topics in Terrorism Research: Reviewing Trends and Gaps, 2007-2016," *Critical Studies on Terrorism* 12, no. 3 (2019): 469.
27. Ines von Behr, Anaïs Reding, Charlie Edwards, and Luke Gribbon, *Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism* (Brussels: RAND Europe, 2013); Paul Gill and Emily Corner, "Lone Actor Terrorist Use of the Internet and Behavioural Correlates," in *Terrorism Online: Politics, Law and Technology*, ed. Lee Jarvis, Stuart MacDonald, and Thomas M. Chen (London: Routledge, 2015), 47–65; Paul Gill, 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, no. 1 (2017): 99–117.
28. Maura Conway, "Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet," *First Monday* 7, no. 11 (2002): 6.
29. Louise Amoore, *The Politics of Possibility: Risk and Security Beyond Probability* (Durham: Duke University Press, 2013), 9.
30. Duncan B. Hollis, "An e-SOS for Cyberspace," *Harvard International Law Journal* 52 (2011): 382.
31. Chad Parks, "Cyber Terrorism: Hype or Reality?", *The Journal of Corporate Accounting and Finance* 14 (2003): 1.
32. Jack M. Balkin, "Free Speech Is a Triangle," *Columbia Law Review* 118, no. 7 (2018): 2011–56.
33. Bill Nelson, Choi Rodney, Michael Iacobucci, Mark Mitchell, and Greg Gagnon, *Cyberterror: Prospects and Implications* (Monterey, CA: Naval Postgraduate School, 1999).
34. Cfr. Stefan Soesanto, *Cyber Terrorism: Why It Exists, Why It Doesn't, and Why It Will* (Madrid: Real Instituto Elcano Royal Institute, 2020).
35. Bill Nelson et al., "Cyberterror," 7.
36. Dale L. Watson, "Testimony before the Senate Select Committee on Intelligence" (Washington, 6 February 2002), https://archives.fbi.gov/archives/news/testimony/the-terrorist-threat-confronting-the-united-states (accessed May 19, 2021).
37. Cfr. Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Broadway Books, 2014), 141.
38. On how Anonymous escaped the terrorist labeling, please see: Gabriella Coleman, *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous* (New York: Verso, 2014).
39. Michael T. McCarthy, "USA Patriot Act," *Harvard Journal on Legislation* 39, no. 2 (2002): 435–54.
40. Cfr. Amitai Etzioni, *How Patriotic Is the Patriot Act?: Freedom versus Security in the Age of Terrorism*. (Abingdon: Routledge, 2005); Michael T. McCarthy, "USA Patriot Act".
41. Amongst these: the "authority to intercept wire, oral, and electronic communications relating to computer fraud and abuse offenses" (§202), "emergency disclosure of electronic communications to protect life and limb" (§212), and "interception of computer trespasser communications" (§217) – Pub. L. No. 107-56, 115 Stat. 272 (2001): https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.htm (accessed May 19, 2021). As indicated in a 2005 report of the Department of Justice, §202 has been however applied only in two occasions, "occurred in a computer fraud investigation that eventually broadened to include drug trafficking" – that is, an instance of cyber-crime.

42. For a comprehensive account of the genealogy of cyber terrorism as a policy domain in the United States, please see Kristzina Hustzi-Orban, "United States and Cyber Terrorism: From Ideological Cradle to the Test of International Standards," in *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, 2020): 6–10.
43. Anne Stenersen, "The Internet: A Virtual Training Camp?," *Terrorism and Political Violence* 20, no. 2 (2008): 215–33; and UNODC, *The Use of the Internet for Terrorist Purposes* (Vienna: UNODC, 2012), https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf (accessed May 19, 2021).
44. An example of international cooperation: Anita K. Jones, Igor Fedorov, Lewis M. Branscomb, Nikolay V. Medvedev, Yury K. Shiyan, Linton Wells III, Michael Wolin, and A. Chelsea Sharber, "Report of U.S.-Russian Working Group on Cyberterrorism Issues," in *Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop*, ed. Glenn E. Schweitzer and A. Chelsea Sharber (Washington, DC: The National Academies Press, 2005), 9–13.
45. United Kingdom Home Office, "Terrorism: Home Secretary's Speech to the Council on Foreign Relations," (16 September 2011) https://www.gov.uk/government/speeches/terrorism-home-secretarys-speech-to-the-council-on-foreign-relations (accessed May 19, 2021).
46. United Kingdom Prime Minister Office, "PM speech at Commonwealth Leaders Reception," (20 September 2017) https://www.gov.uk/government/speeches/pm-speech-at-commonwealth-leaders-reception (accessed May 19, 2021).
47. Cfr. Claudia Aradau and Rens van Munster, "The Next Terrorist Attack" and "Securing Catastrophic Futures," *Politics of Catastrophe: Genealogies of the Unknown* (Abingdon: Routledge, 2011), 17–30.
48. Cfr. Stuart Macdonald, Lee Jarvis, and Simon M. Lavis, "Cyberterrorism Today? Findings From a Follow-On Survey of Researchers," *Studies in Conflict & Terrorism* (2019): 1–26; and Tim Stevens, "Strategic Cyberterrorism: Problems of Ends, Ways and Means," in *Handbook of Terrorism and Counter Terrorism Post 9/11*, eds. David Martin Jones, Paul Schulte, Carl Ungerer, and Michael L. R. Smith (Cheltenham: Edward Elgar Publishing, 2019), 42–52.
49. *National Cyber Strategy of the United States of America* (September 2018), https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (accessed May 19, 2021).
50. On the construction of cyber terrorism as a threat in the United Kingdom, please see Gareth Mott, *Constructing the Cyberterrorist: Critical Reflections on the UK Case* (Abingdon: Routledge, 2019) and Gareth Mott, "United Kingdom: The Constructed Threat of Cyber Terrorism," in *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, 2020): 11–15.
51. United Kingdom Prime Minister Office, *National Security Strategy and Strategic Defense and Security Review 2015* (23 November 2015). https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015 (accessed May 19, 2021).
52. United Kingdom Prime Minister Office, *National Cyber Security Strategy 2016 to 2021* (1 November 2016), https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 (accessed May 19, 2021).
53. Ibid., 19.
54. Ibid., 48.
55. Ibid., 17.
56. Ibid., 50.
57. Ibid., 51.
58. Cfr. François Delerue, Alix Desforges, and Aude Géry, "A Close Look at France's New Military Cyber Strategy," *War on the Rocks* (23 April 2019), https://warontherocks.com/2019/04/a-close-look-at-frances-new-military-cyber-strategy/ (accessed May 19, 2021).

59. *French National Digital Security Strategy* (2015), 14, https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf (accessed May 19, 2021).
60. On China's policies on cyber terrorism, please see Siodhbhra Parkin, "China: The 'Three Evils' of Cyberspace and Human Rights," in *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, 2020): 16–20.
61. *Criminal Law of the People's Republic of China* (2015), http://english.court.gov.cn/2015-12/01/content_22595464_26.htm# (accessed May 19, 2021).
62. *Counterterrorism Law of the People's Republic of China* (2016), https://www.uschina.org/china-hub/unofficial-translation-counter-terrorism-law-peoples-republic-china (accessed May 19, 2021).
63. *Cybersecurity Law of the People's Republic of China* (2017), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/ (accessed May 19, 2021).
64. Cfr. M. Clarke (ed.), *Terrorism and Counter-Terrorism in China: Domestic and Foreign Policy Dimensions* (Oxford University Press, 2018).
65. *Overview of China's Cybersecurity Law* (KPMG China, February 2017), https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf (accessed May 19, 2021).
66. James Leibold, "Surveillance in China's Xinjiang Region: Ethnic Sorting, Coercion, and Inducement," *Journal of Contemporary China* 29, no. 121 (2020): 46–60.
67. Sergei Petrenko, *Big Data Technologies for Monitoring of Computer Security: A Case Study of the Russian Federation* (Cham: Springer, 2018), 1–249.
68. Ibid., article 43. On this issue, please see Eva Claessen, "Russia: Cyber Terrorism as an Issue of Information Security," in *Countering Cyber Terrorism in a Time of 'War on Words' Kryptonite for the Protection of Digital Rights?* (The Hague Program for Cyber Norms, 2020): 21–27.
69. *Russian Federation's Doctrine for Information Security* (2016–2017), https://publicintelligence.net/ru-information-security-2016/ (accessed May 19, 2021).
70. Ibid., ¶1.
71. On the relationship between effects and intents peculiar to the war on terror doctrines, please see Marieke De Goede, *Speculative security: The politics of pursuing terrorist monies* (University of Minnesota Press, 2012).
72. Cfr. Sarah Brayne and Angèle Christin, "Technologies of Crime Prediction: The Reception of Algorithms in Policing and Criminal Courts," *Social Problems* (2020): 1–17; Barton Gellman, *Dark Mirror: Edward Snowden and the American Surveillance State* (Random House, 2020); Robert Gorwa, Reuben Binns, and Christian Katzenbach, "Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance," *Big Data & Society* 7, no. 1 (2020): 1–15.
73. See Clive Walker, "The War of Words with Terrorism: An Assessment of Three Approaches to Pursue and Prevent," *Journal of Conflict and Security Law* 22, no. 3 (2017): 523–551; Eugénie Coche, "Privatized Enforcement and the Right to Freedom of Expression in a World Confronted with Terrorism Propaganda Online," *Internet Policy Review* 7, no. 4 (2018): 1–17; and Sarah Brayne's forthcoming *Predict and Surveil* (Oxford: Oxford University Press).
74. Cfr. Danielle Keats Citron, "Extremist Speech, Compelled Conformity, and Censorship Creep," *Notre Dame L. Rev.* 93, no. 3 (2017): 1035–72.
75. United Kingdom Parliamentary Joint Committee on Human Rights, "Amendment of Terrorist Offences," *Legislative Scrutiny: Counter-Terrorism and Border Security Bill* (July 2018), https://publications.parliament.uk/pa/jt201719/jtselect/jtrights/1208/1208.pdf (accessed May 19, 2021).
76. United Kingdom Home Office, *Online Harms White Paper* (2020), https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper (accessed May 19, 2021).

77. Graham Smith, "Online Harms and the Legality Principle," *Cyberleagle* (blog post, 20 June 2020), https://www.cyberleagle.com/2020/06/online-harms-and-legality-principle.html (accessed May 19, 2021).
78. For an overview of France's domestic debate on terrorism and cyberspace, please see Rebecca Mignot-Mahdavi, "France: Issues of Form and Substance in the National Strategy of Terrorist Threat Anticipation in Cyberspace," in *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, 2020): 28–34.
79. European Commission, "Regulation of the European Parliament and of the Council on preventing the Dissemination of Terrorist Content Online" (September 2018), https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52018PC0640 (accessed May 19, 2021). The Commission's policy proposal envisions a number of far-reaching provisions: "a legally binding one-hour deadline for content to be removed following a removal order from national competent authorities"; "definition of terrorist content as material that incites or advocates committing terrorist offences, promotes the activities of a terrorist group or provides instructions and techniques for committing terrorist offences"; "a duty of care obligation for all platforms to ensure they are not misused for the dissemination of terrorist content"; "a framework for strengthened co-operation between hosting service providers, Member States and Europol"; and "effective complaint mechanisms that all service providers will have to put in place".
80. UNHR's Office of the High Commissioner, "UN human rights experts concerned about EU's online counter-terrorism proposal" (12 December 2018), https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=24013&LangID=E (accessed May 19, 2021).
81. The final text of the legislation can be retrieved here: https://data.consilium.europa.eu/doc/document/ST-14308-2020-REV-1/en/pdf (accessed May 19, 2021). It now includes a number of safeguards addressing some of the criticism raised in the past years. Amongst the others, it now states that "material disseminated for educational, journalistic, artistic or research purposes or for awareness-raising purposes against terrorist activity should not be considered to be terrorist content". However, the contested one-hour removal time has been confirmed. On this topic, please see 'EU adopts law giving tech giants one hour to remove terrorist content', https://www.euractiv.com/section/cybersecurity/news/eu-adopts-law-giving-tech-giants-one-hour-to-remove-terrorist-content/ (accessed May 19, 2021).
82. For a broader overview of the EU's take on cyber terrorism, please see Stef Wittendorp, "European Union: The Narrative Implications of Conceptualizing 35 Cyber Terrorism as a Threat," in *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, 2020): 35–38.
83. French Republic's National Assembly, "LOI n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet (1)" (25 June 2020), https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042031970 (accessed May 19, 2021).
84. French Republic's Constitutional Court, "Décision n° 2020-801 DC du 18 juin 2020" (25 June 2020), https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042031998/ (accessed May 19, 2021).
85. *The Christchurch Call* (2019), full text available at: https://www.christchurchcall.com/call.html (accessed May 19, 2021).
86. The full list of the call's supporters can be consulted at: https://www.christchurchcall.com/supporters.html (accessed May 19, 2021).
87. *The Christchurch Call* builds, and makes extensive reference, to a similar initiative launched by the United Kingdom. Following the Westminster terrorist attack in March 2017, the government convened a roundtable with major industry players, including Facebook, Twitter, Google and Microsoft to see what more could be done to tackle terrorist content online. This led to these companies setting up the Global Internet Forum to Counter Terrorism (GIFCT) in June 2017.

88. The White House's Office of Science and Technology Policy, "Statement on Christchurch Call for Action" (US Embassy & Consulate in New Zealand, Cook Islands, and Niue, 15 May 2019), available at: https://nz.usembassy.gov/statement-on-christchurch-call-for-action/ (accessed October 1, 2020).
89. Anastasia Tolstukhina, "Global Tech Companies Counter Online Terrorist Content", *Russian International Affairs Council* (2 April 2020), https://russiancouncil.ru/en/analytics-and-comments/analytics/global-tech-companies-counter-online-terrorist-content/ (accessed May 19, 2021).
90. Human Rights Watch (HRW), "Russia: Growing Internet Isolation, Control, Censorship" (18 June 2020), https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship (accessed May 19, 2021). As further explained by HRW, these laws and regulations effectively reinforce a draft of laws adopted in previous years that enable the authorities to unjustifiably ban a wide range of content. Since 2017, the government has also increased the number of official agencies with powers to order content blocking, and increased the fines for organizations, including internet service providers, proxy services, and search engines, that refuse to take down such content or that provide means to circumvent content blocking.
91. Cyberspace Administration of China, *National Cyberspace Security Strategy* (27 December 2017), http://www.cac.gov.cn/2016-12/27/c_1120195926.htm (accessed May 19, 2021).
92. Cfr. International Federation for Human Rights, *China's New Counter-terrorism Law: Implications and Dangers for Tibetans and Uyghurs* (November 2016), https://www.refworld.org/docid/582b119b4.html (accessed May 19, 2021).
93. Human Rights Watch, "China: Draft Counterterrorism Law a Recipe for Abuses" (20 January 2015), https://www.hrw.org/news/2015/01/20/china-draft-counterterrorism-law-recipe-abuses (accessed May 19, 2021).
94. Human Rights Watch, "China: Disclose Details of Terrorism Convictions" (16 March 2017), https://www.hrw.org/news/2017/03/16/china-disclose-details-terrorism-convictions (accessed May 19, 2021).
95. See Caitriona Heinl, "Terrorist Access to Offensive Cyber Means and How This Threat Might Be Best Managed," in *Oxford Handbook of Cyber Security*, ed. Paul Cornish (Oxford University Press, 2020/forthcoming) for an overview, see also "An Initial Overview of UN System Actors, Processes and Activities on ICT-Related Issues of Interest to the OEWG, by Theme" (January 2020), https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/background-paper-on-existing-un-bodies-processes-related-to-mandate.pdf (accessed May 19, 2021).
96. UNGA, A/65/201 *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE 2010)* (New York: UN, 2010); UNGA, A/68/98 *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE 2013)* (New York: UN, 2013); UNGA, A/70/174 *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE 2015)* (New York: UN, 2015).
97. For background on this split in the process see Tim Maurer, "A Dose of Realism: The Contestation and Politics of Cyber Norms," *Hague Journal of the Rule of Law* 12 (2019): 1–23; Dennis Broeders and Bibi van den Berg, "Governing Cyberspace. Behavior, Power, and Diplomacy," in *Governing Cyberspace. Behavior, Power, and Diplomacy*, eds. Dennis Broeders and Bibi van den Berg (London: Rowman and Littlefield, 2020), 1–15.
98. See US resolution: UNGA, A/C.1/73/L.37 *Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* (18 October 2018), https://undocs.org/A/C.1/73/L.37 (accessed May 19, 2021).
99. See Russian resolution: UNGA, A/C.1/73/L.27/Rev.1 *Developments in the Field of Information and Telecommunications in the Context of International Security* (29 October 2018), https://undocs.org/A/C.1/73/L.27/Rev.1 (accessed May 19, 2021).

100. Moreover, the UN GGE is a process where the report is negotiated by 'governmental experts' which strictly speaking means that it is not a formal negotiation between states. The OEWG in contrast is open to the participation of all UN member states in their capacity as state representatives. The contributions to the OEWG are therefore formally state positions and do not have the (im)plausible deniability of them being an expert position.
101. UNGA, A/RES/53/70 *Developments in the Field of Information and Telecommunications in the Context of International Security* (New York: UN, 1999).
102. Xymena Kurowska, "What Does Russia Want in Cyber Diplomacy? A Primer," in *Governing Cyberspace. Behavior, Power, and Diplomacy*, eds. Dennis Broeders and Bibi van den Berg (London: Rowman and Littlefield, 2020), 85–106; Dennis Broeders, 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).
103. Rogier Creemers, "China's Conception of Cyber Sovereignty: Rhetoric and Realization," in *Governing Cyberspace. Behavior, Power, and Diplomacy*, eds. Dennis Broeders and Bibi van den Berg (London: Rowman and Littlefield, 2020), 107–44; Broeders, Adamson and Creemers, "Coalition of the unwilling".
104. Hillary Rodham Clinton, "Remarks on Internet Freedom" (Washington, DC: US Department of State, 2010), https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm (accessed May 19, 2021).
105. Cfr. UNHRC, A/HRC/41/35 *Surveillance and human rights: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* (28 May 2019), https://undocs.org/A/HRC/41/35 (accessed May 19, 2021).
106. See for example: Ronald Deibert, *Black Code. Inside the Battle for Cyber Space* (Toronto: Signal, 2013); Laura DeNardis, *The Global War for Internet Governance* (New Haven and London: Yale University Press, 2014); Dennis Broeders, *The Public Core of the Internet: An International Agenda for Internet Governance* (Amsterdam: Amsterdam University Press, 2015); Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York: Public Affairs, 2016).
107. Petter Nesser, Anne Stenersen, and Emilie Oftedal, "Jihadi Terrorism in Europe: The IS-Effect," *Perspectives on Terrorism* 10, no. 6 (2016): 3–24; Imran Awan, "Cyber-Extremism: Isis and the Power of Social Media," *Society* 54, no. 2 (2017): 138–49; Haroro J. Ingram, "An Analysis of Inspire and Dabiq: Lessons from AQAP and Islamic State's Propaganda War," *Studies in Conflict & Terrorism* 40, no. 5 (2017): 357–75; Roel de Bont, Daan Weggemans, Ruud Peters, and Edwin Bakker, "Life at ISIS: The Roles of Western Men, Women and Children," *Security and Global Affairs* (2017): 3–17.
108. *UN GGE 2010*; *UN GGE 2013*; *UN GGE 2015*.
109. *UN GGE 2010*, 6–7.
110. *UN GGE 2013*, 7
111. Ibid., 8, 10.
112. *UN GGE 2015*: 6.
113. Ibid., 10.
114. Ibid., 10–11.
115. Ibid., 13–14.
116. For an overview of OEWG's planned activities and resources, please see UNODA's website: https://www.un.org/disarmament/open-ended-working-group/ (accessed May 19, 2021).
117. Final Substantive Report of the report of the OEWG on developments in the field of information and telecommunications in the context of international security. 10 March 2021. https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf (accessed May 19, 2021).
118. *Initial Pre-draft of the report of the OEWG on developments in the field of information and telecommunications in the context of international security* (27 April 2020), https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/03/200311-Pre-Draft-OEWG-ICT.pdf (accessed May 19, 2021).

119. Russian Federation's commentary on the OEWG's initial pre-draft (April 2020), 1, https://front.un-arm.org/wp-content/uploads/2020/04/russian-commentary-on-oweg-zero-draft-report-eng.pdf (accessed May 19, 2021).
120. China's commentary on the OEWG's initial pre-draft (April 2020), 1-2, https://front.un-arm.org/wp-content/uploads/2020/04/china-contribution-to-oewg-pre-draft-report-final.pdf (accessed May 19, 2021).
121. Ibid., 5.
122. Ethan Zuckerman, "Intermediary Censorship," in *Access Controlled. The Shaping of Power, Rights, and Rule in Cyberspace*, eds. Ronald Deibert, Johan Palfrey, Rafal Rohozinski, and Jonathan Zittrain (Cambridge, MA: MIT Press, 2010), 71–85.
123. Tarleton Gillespie, "Platforms Are Not Intermediaries," *Georgetown Law Technology Review* 2, no. 2 (2018): 198–216; Robert Gorwa, "What Is Platform Governance?," *Information, Communication & Society* 22, no. 6 (2019): 854–71.
124. Australia's commentary on the OEWG's initial pre-draft (16 April 2020), https://front.un-arm.org/wp-content/uploads/2020/04/final-australia-comments-on-oewg-pre-draft-report-16-april.pdf (accessed May 19, 2021).
125. Venezuela's commentary on the OEWG's initial pre-draft (April 2020), 3, https://front.un-arm.org/wp-content/uploads/2020/04/nv-00069-annex.pdf (accessed May 19, 2021).
126. Zimbabwe's commentary on the OEWG's initial pre-draft (April 2020), 1–2, https://front.un-arm.org/wp-content/uploads/2020/04/zimbabwe-position-on-pre-draft-of-oweg-final-report.pdf (accessed May 19, 2021).
127. Islamic Republic of Iran's commentary on the OEWG's initial pre-draft (April 2020), https://front.un-arm.org/wp-content/uploads/2020/04/iran-preliminary-on-oewg-pre-draft-15-april-2020-1.pdf (accessed May 19, 2021).
128. NAM's commentary on the OEWG's initial pre-draft (April 2020), 2, https://front.un-arm.org/wp-content/uploads/2020/04/nam-wp-to-the-oewg-final.pdf (accessed May 19, 2021).
129. Tim Maurer, "Dose of Realism", 5.
130. Dennis Broeders, "Creating Consequences for Election Interference," *Directions. Cyber Digital Europe* (15 May 2020), https://directionsblog.eu/creating-consequences-for-election-interference/ (accessed May 19, 2021).
131. France's commentary on the OEWG's initial pre-draft (April 2020), https://front.un-arm.org/wp-content/uploads/2020/04/contribution-fr-oewg-eng-vf.pdf (accessed May 19, 2021).
132. The Kingdom of the Netherlands' commentary on the OEWG's initial pre-draft (April 2020), https://front.un-arm.org/wp-content/uploads/2020/04/kingdom-of-the-netherlands-response-pre-draft-oewg.pdf (accessed May 19, 2021).
133. Final Substantive Report of the report of the OEWG on developments in the field of information and telecommunications in the context of international security. 10 March 2021, page 3. https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf (accessed May 19, 2021).
134. Chair's Summary of the OEWG on developments in the field of information and telecommunications in the context of international security. 10 March 2021. https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf (accessed May 19, 2021).
135. For a more detailed analysis of the current OEWG and UN GGE, as well as the coming UN processes, see: Dennis Broeders, "The (im)possibilities of addressing election interference and the public core of the internet in the UN GGE and OEWG: a mid-process assessment", *Journal of Cyber Policy*, (2021), DOI: 10.1080/23738871.2021.1916976
136. As shown in the HRW's reports on China and Russia cited in this article, the vagueness of national policies' language concerns the boundaries of concepts such as hate, extremism, social unity, harassment, etc. A similar debate has emerged around social media platforms' liability in implementing vague standards for content moderation. On this, please see the section "Areas of concern around content standards" in UNHRC, A/HRC/38/35 *Report of the Special Rapporteur on the promotion and protection of the right*

to freedom of opinion and expression (6 April 2018), 10–12, https://undocs.org/A/HRC/38/35 (accessed May 19, 2021).

137. See fore example: Nicholas Tsagourias, "Electoral Cyber Interference, Self-Determination, and the Principle of Non-Intervention in Cyberspace," in *Governing Cyberspace: Behaviour, Power and Diplomacy*, eds. Dennis Broeders and Bibi van den Berg (London: Rowman & Littlefield, 2020), 45–63; Jens Ohlin, *Election Interference. International Law and the Future of Democracy* (Cambridge: Cambridge University Press, 2020).

ORCID

Dennis Broeders http://orcid.org/0000-0002-8827-2814
Fabio Cristiano http://orcid.org/0000-0002-0951-9648
Daan Weggemans http://orcid.org/0000-0003-3039-5579