The End of Self-Regulation: On the Role of Internet Intermediaries in Countering Terror

Raphael COHEN-ALMAGOR[1]
University of Hull

Abstract. Terrorism is a significant concern worldwide. Criminals, jihadists, and terrorists are quick to use technology to protect their anonymity, privacy, modes of operation, and secret antisocial plans. They adapt to new innovations and exploit any technological advantages as means to ends. Clandestine operations are used to raise funds. Criminals, jihadists, and terrorists are working in international cells and rings that contest geographical boundaries and that require large resources and international security cooperation to obstruct their activities. Addressing these cross-country challenges require cross-country cooperation. The aim of this essay is to analyze the role of Internet intermediaries in countering online terror. I argue that Internet intermediaries can and should do far more than what they do to proactively fight online terrorism and that self-regulation is not effective enough. It is time for governments to step in and to protect vulnerable third parties by demanding that Internet intermediaries be vigilant and proactive in fighting terror. The idea of a new browser, CleaNet, is proposed to ensure a safe environment for Net users and for society at large.

Keywords: CleaNet, Internet, ISPs, jihad, social responsibility, terror, violence

Introduction

The Internet burst into our lives in the early 1990s without much preparation or planning and changed our lives forever. Virtually every aspect of society was affected by this macro system of interconnected private and public networks: household, literary, military, academic, artistic, business, and government. The Internet has produced major leaps forward in human productivity and has changed the way people work, study and interact with each other. The mix of open standards, diverse networks, and the growing ubiquity of digital devices undermines traditional media and challenges existing regulatory institutions based on national boundaries. The Internet has created new markets and has changed the way people interact, find leisure, explore the world, and think about human phenomena. In the Internet age, people often have a cyber life in addition to their offline life. The two lives—real and cyber—are not necessarily one and the same.

The object of this essay is to address the ethical problems rooted in cyber technology by considering how best to respond to potential violent risks on the Internet. The Internet

[1] Corresponding Author: Raphael Cohen-Almagor. E-mail: almagor35@gmail.com . The author is grateful to Jack Goldstone and the participants of the NATO *The Post ISIS-era: Regional and Global Implications* workshop for their incisive remarks and criticisms.

itself, however, is not the problem. Problems arise when the Internet is used to undermine our well-being as autonomous individuals living in free societies. This study focuses on articulating possible solutions to specific problems and providing a framework within which these problems can be identified and resolved by accentuating the concepts of moral and social responsibility.

Section I explains key terms: terrorism and counterterrorism, jihad and e-jihad, corporate social responsibility (CSR), Netuser and Netcitizen, and deliberative democracy. Section II discusses the relationships between jihad and terror. Section III elucidates the expected responsibilities of Internet intermediaries. While having codes of conduct is important, it is no less important to enforce them; if not enforced, such codes become no more than dead dogma. I also recommend the creation of active cyber patrols to search for and remove violent content; the creation of hotlines that enable easy reporting of violent expressions; improved machine learning; close monitoring of terrorist websites; and using Stop! messages to invite readers' reflections. Section IV argues that states should step in and enforce efficient Internet regulation to prevent further abuse and loss of life. Finally, Section V presents CleaNet, a new browser that attempts to balance between freedom of expression and social responsibility.

1. Definitions

The word *terror* comes from the Latin "terrere," meaning "to frighten" or "to scare" [1]-[4]. *Terrorism* is defined as the threat or use of violence against noncombatant targets for political, religious or ideological purposes by subnational groups and/or clandestine individuals who are willing to justify all means to achieve their goals.[2] Terrorist conduct is designed to attract attention to the terrorist's cause and to spread fear and anxiety among wide circles of the targeted population. Terrorist motivation is customarily devoid of personal gain. It usually is political, religious, or ideological. Acts of terror typically are the work of a small number of committed individuals who strive for what they perceive as the "greater good" of a larger group with whom the terrorists identify. Terrorists are willing to break any rule to promote their ends. International conventions do not apply to them. Breaking all norms and rules is the guiding rule for terrorists. Their means may have no limits. Terrorists often are willing to justify all means to achieve their goals and to use violence or the threat of violence against their targets. Any person who does not belong to the terrorist group or its allies is potentially included in the general category of "the enemy." The targets of terrorists include noncombatants, innocent civilians, and representatives of the state. Any location may be regarded as a legitimate locus for destruction. Terrorists want to surprise, keep the enemy on its toes, exhaust, instil fear, and stretch the enemy's resources. They attack anywhere they can [5].

Until now, the international community has failed to agree on a definition of terrorism. Lack of such a definition helps terror organizations, as resources that could have been mobilized against terror activities are not made available, and international cooperation, which is essential for combatting international terrorism, is deficient. The

[2] For a discussion on the complicated task of defining terrorism, see Schmid, A. P. (2011). The definition of terrorism. In in A.P. Schmid (Ed.), *The Routledge handbook of terrorism research: research, theories and concepts* (pp. 39-98). (London, England: Routledge; and Martin, G. (2011). *Essentials of terrorism* (pp. 2-25). Thousand Oaks, CA: SAGE.

Council of Europe Committee of Counter-Terrorism understands this shortcoming and is seeking to reach a definition that would be accepted by all or most member states. It is hoped that by 2021, the Council of Europe will adopt such a binding definition [6].

Counterterrorism is defined as proactive and offensive measures taken to prevent, deter, forestall, minimize, disturb, and respond to terrorism. These measures can be military or nonmilitary. Nonmilitary measures include legal, psychological, and sociological attempts to punish the perpetrators of terrorist attacks, trace and deradicalize potential terrorists, and decrease intercultural prejudice, which might breed and encourage terrorist violence [7], [8].

The literal meaning of *jihad* is "struggle, strive or effort." Muslims use the word jihad to describe four different kinds of struggle: (1) jihad nafsii (self-improvement), (2) jihad shaitani (struggle with the devil), (3) jihad al-kufar (struggle against the infidel), and (4) jihad al-munafikin (struggle against hypocrites). Jihad nafsii and jihad shaitani, the two major forms of jihad, are personal and internal and refer to the believer's inner struggle to live out the Muslim faith. Each Muslim, for example, is expected to fight the evil temptations in the person's heart. Spiritual jihad is an onerous task and is referred to as the Great Jihad. Jihad al-kufar and jihad al-munafikin are external and collective. These two forms of Small Jihad are distinctly militant and coercive. They are concerned with the struggle to build a good Muslim society, a struggle that may involve the right and the duty to check upon fellow Muslims and to bring them back into line. Small Jihad may necessitate Holy War, which can be described as the perpetual struggle to defend Islam with violence and force if necessary. Holy War instructs believers to fight against infidels and those who defy Islam and to expand Islam in the world [9], [10].

The Quran states that "Truly God defends those who have faith. Truly God loves not the treacherous rejecter [kafir]. Permission [for warfare] is given to those who are attacked and definitely wronged. And truly God is capable of helping without justice" (22:38-41) [11]. Radical Muslims urge jihadists to take up arms in the jihad to repel the infidels. Thus, jihadism is a branch of political Islam that aims, through armed fights and war (jihad), to bring about the rule of Islam and the establishment of the Caliphate (Islamic) State in different parts of the world. In recent decades, jihadism has developed on the basis of a specific interpretation of Salafist doctrine and the radical ideas of Sayyid Qutb.[3]

The term *e-jihad* refers to the way that groups such as al-Qaeda and ISIS use information technology (e.g., email and encrypted files) to organize the logistics for their campaigns and develop strategic intelligence [12].

Corporate social responsibility refers to integrity in business. CSR calls for integrated, sustainable decision-making that takes into consideration the positive and negative potential consequences of decisions; obligates corporations to not only consider different stakeholders and interests but also to incorporate those stakeholders and interests into the decision-making process; stresses that transparency is vital for ensuring accountability to stakeholders; and demands the acceptance of liability for decisions and the enactment of remedial measures to redress harm inflicted as a result of the corporation's conduct [13]-[16].

---

[3] For more information on the Salafi doctrine, see Meijer, R. (Ed.). (2009). *Global Salafism: Islam's new religious movement*. New York, NY: Columbia University Press. For more information on Sayyid Qutb, see Calvert, J. (2010). *Sayyid Qutb and the origins of radical Islamism*. New York, NY: Columbia University Press; Bergesen, A. J. (Ed.). (2007). *The Sayyid Qutb reader: Selected writings on politics, religion, and society*. New York, NY: Routledge; and Akerboom, E. S. M. (Ed.). (2009). *Ideology and strategy of jihadism*. The Hague National Coordinator for Counter-Terrorism: The Hague, Netherlands.

In this context, it is important to distinguish between *legal* liability and *moral* liability. Under the European Union's e-commerce directive, Internet platforms are protected from *legal* liability for any illegal content they "host" (rather than create) until they have either actual knowledge of the illegal content or are made aware of facts or circumstances from which it would have been apparent that the content was unlawful and failed to act "expeditiously" to remove or disable access to such content. The existing liability requirements under the e-commerce directive therefore force companies to act against illegal content only after they have been notified of its existence [17]. Internet intermediaries, however, are still *morally* liable for failure to be proactive about ensuring a safe environment for users. Archie Carroll articulated in his seminal work that beyond the obvious economic and legal obligations that a firm has, the social responsibility of businesses also encompasses ethical and discretionary responsibilities. Businesses are expected, by definition, to make a profit, and society expects businesses to obey the law. According to Carroll, ethical responsibilities include adherence to the ethical norms of fairness, justice, and due process, while discretionary responsibilities include making philanthropic contributions and engaging in nonprofit social welfare activities [18]-[20]. Carroll's pyramid of CSR has economics as the base and builds upward through legal, ethical, and philanthropic categories. In Carroll's view, companies that practice good CSR strive to make a profit while obeying the law and behaving ethically as good corporate citizens [21]-[23].

Gatekeeping is defined as the work of third parties who are able to disrupt misconduct by withholding their cooperation from wrongdoers [24]. As gatekeepers, it is argued, Internet intermediaries need to be far more proactive than they are now. Socially responsible measures can prevent the translation of violent thoughts into violent actions. Designated monitoring mechanisms can potentially prevent such unfortunate events.

The term *Netuser* refers to people who use the Internet. It is a neutral term. It does not convey any clues about how people use the Internet. It does not suggest any appraisal of those uses. In contrast, the term *Netcitizen*, as it is used here, is not neutral. It describes the *responsible* use of the Internet. While it is possible to speak of "good" and "bad" citizens, the term Netcitizen, as used here has only positive connotations and refers to concerned Internet users who access the Net for positive, socially responsible, and non-abusive purposes and are willing to be proactive in promoting an Internet environment that is safe to use as an integral part of their real lives. Netcitizens make no distinction between their virtual lives and their real lives and act uprightly in both realms. Netcitizens are good citizens of the Internet. They contribute to the use and growth of the Internet while trying to ensure that their communications and Net use are constructive. They foster free speech, open access, and a social culture that focuses on respecting others rather than harming them. Netcitizens are Netusers with a sense of responsibility [25].[4]

Deliberative democracy refers to a process in which self-government extends to collective self-government. Deliberative democracy evokes ideals of rational legislation, of participatory politics, and of civic self-governance and autonomy. It presents an ideal of political autonomy based on the practical reasoning expressed in an open and accountable discourse, leading to an agreed judgment on substantive policy issues concerning the common good. Deliberative

[4] For further discussion, see Nerlich, B., Hartley, S., Raman, S., & Smith, A. (Eds.). (2018). *Science and the politics of openness*. Manchester, England: Manchester University Press.

discourse is un-coerced, pluralistic, inclusive, and reasoned. It is aimed to shape the common interests of participating citizens [26]-[32]. People weigh considerations, consolidate judgments, and convey their reasons for a particular course of action. Public discussion is perceived to be a common good. People address the problems they are facing together. As members of the same polity, they assume that they have common interests and that they will be able to reach agreement on principles and policies. Political leaders have a moral obligation and a moral responsibility to tease out just, reasonable policies through the mechanisms of compromise and deliberation while showing respect for and acknowledgment of plural interests and expressing a sincere desire to reach a consensus or at least a mutually satisfactory agreement. Respect for different perceptions of the common good and a commitment to moderation must be promoted.

2. Jihad and Terror

Modern terrorism relies heavily on the Internet. Both modern terrorism and the Internet have common features that promote close relations: they are global and diffuse; they do not necessarily require one center; their operations do not require a large budget; innovation is important to their sustainability; and operations can be enabled by clandestine means. Terrorists and their abettors and collaborators strive to keep their identity, their modes of operation, and their plans secret. They use advanced technological tools to secure their privacy and anonymity and are quick to adapt to new innovations and exploit any and all technological advantages as means to ends. Clandestine modes of operation generate the funds needed to pursue their goals. Terrorists work in international cells and rings that contest geographical boundaries and that require extensive resources and close cooperation among law-enforcement agencies from different countries to obstruct the terrorists' activities.

The Internet has enabled a global jihad based on a loose, decentralized network of Mujahideen transcending the limitations of face-to-face interactions [33], [34]. E-mails and chats are as popular among radicals and terrorists as they are among other Netusers. Terrorists, like people who use the Internet for social purposes, use the vast information available on the Internet to coordinate, communicate, share know-how (e.g., bombmaking, suicide bombing, guerrilla operations), and find essential data for waging antisocial, violent operations. Terrorists abuse the Internet to legitimize their violent ideas, disseminate their ideology, spread jihadist and terrorist propaganda, appeal for support, evoke fear and alarm among their foes, radicalize interested parties, provide instruction on tactics and weapons, gather intelligence about potential targets, communicate clandestinely, and support terrorist operations [17]. The Internet assists E-jihad and E-terror. It enables terrorist organizations to expand their reach, create virtual communities of like-minded extremists, capture a larger universe of more-diverse talents and skills, clandestinely raise funds for terrorist operations, and to recruit globally for taking part in jihadi battles and terrorist operations [35]-[38].

Many terrorists begin their journey to violent jihad on the Internet, seeking solutions to personal crises, validation and reinforcement of their anger, and the thrill of clandestine participation in an epic struggle [39], [40]. Radical forums create virtual communities, connect like-minded people, provide rich information on timely topics, reinforce beliefs, and normalize violent behaviour. Thousands of websites and bulletin boards offer videos, images, statements, and speeches that demonstrate the Internet's centrality to global terrorism. Great reverence is paid to the views of militant leaders.

Anti-Western videos showing non-Muslims humiliating Muslims populate the Internet in order to win the hearts and minds of potential followers.

Most jihadi websites have several sections. Most important usually is the religious section, which features Quranic references to jihad, the different ways jihad can be expressed, aspects of martyrdom, fatawa (singular is fatwa, a religious edict provided by a Muslim sage) explaining who can be targeted legitimately, and online doctrinal consultations with religious sages. In the jihad section, would-be recruits are encouraged to join the battle. Some general advice is given (e.g., the best routes into war zones; names and locations of sympathetic mosques). Portrait galleries of martyrs are accompanied by their last testaments, often in a video clip. Most sites have an Internet technology section where contributors "are urged to share their knowledge and develop new ways of using cyberspace to further jihad." Online forums and "chatrooms are very popular among jihadi Netusers [41]-[44]. It is very easy to create private chatrooms in which Netusers can post messages for friends and colleagues." Advice can be found on which chatroom to use and the users can interact freely. Communication can be made from any Internet cafe in the world. Interactive technology enables visitors to add comments and reply to ongoing discussions.

Many jihadi websites have a women's section where wives and mothers are urged to support their men in jihad and help them in the psychological battle against what one site described as "that disease," "the weakness which loves life and hates death" [42].

The dark Internet is a home to illicit jihadi information and communication. Jihadi websites allow isolated young Muslims to engage with a worldwide network of like-minded people striving against what they perceive as a common enemy and with a singular unity of purpose [42], [45]. Young Muslim men and women share their hopes and dreams with their virtual friends on these radical forums. Some might have joined a given forum out of a sense of alienation, of feeling alone. It is estimated that hundreds of jihadist forums and websites exist [46]. The forums, where people seem to care for each other, provide members with friends and support. The forums prove the existence of the ummah, or imagined Muslim community [47]. Among the popular jihadi forums were/are: al-Qimmah, Atahadi, al-Jihad al-Alami, al-Fajr, al-Fida al-Islam (no longer active), al-Furqan, al-Faloja (no longer active), al-Hanein, Al-Luyuth al-Islamiyyah, al-Maark, al-Malahem, al-Medad, al-Shamukh, at-Tahaddi, as-Ansar, Hanein, Ansar al-Mujahideen, and The Mujahideen Electronic Network. Some of these are very large, comprising tens of thousands of people. The now-defunct forum www.shawati.com at one point had more than 31,000 registered members. The forum www.kuwaitchat.net, also now defunct, had more than 11,000 registered members [48]-[50]. It is estimated that some 25,000 jihadists originating from more than 100 countries constitute the hard core of jihadi Internet forums [46].[5]

A range of technologies exists that may help in combating online terrorism. Remote surveillance can be used to analyze network traffic, capture and extract Internet protocol (IP) addresses, and access websites, email addresses, server passwords, and graphic- and video-file transfers [51]. Data-linking applications can enable security agencies to share data, cross-reference evidence, identify common patterns, link investigations, and analyze conduct on social networks.

[5] Zelin [49] estimates the number of active jihadi forums in 2012 to be three to five.

3. Responsibility of Internet Intermediaries

Internet intermediaries are gatekeepers and thus bear responsibility for their conduct. The Internet brings together like-minded people and creates a forum for them to discuss and exchange ideas. While the Internet is not the cause of terrorism, it does support and accelerate terror. There are many incidents in which people engage in conversations in chat rooms about jihadi issues because they want to learn about jihad. In these chat rooms, they converse about Islam, jihad, Iraq, Syria, ISIS, Israel-Palestine, and the like. The scope of this phenomenon is broad. Many of these chat-room participants are young Muslims. Their knowledge of Islam is often limited. They are emotionally driven by images from Iraq, Syria, and Palestine. Through the chats, some of them become deeply motivated and radicalized [52].

We are living in an age of terrorism and political violence. The recent surge in terrorism has been aided by the Internet. Attempts to reduce the level of terrorism should include reducing opportunities provided by the Internet to access terrorist information. The electronic environment is more than incidental to terrorist behavior; rather, it shapes behavior and influences conduct. The Internet has frustrated security agencies as it has greatly increased the amount of terrorist information available and the number of individuals accessing that information. Individuals with an active interest in the jihadi movement can easily access propaganda and inciting material and images they crave [53]. Reading violent messages and viewing terror images ignites and strengthens their interest in violent activities. As FBI Associate Executive Assistant Director Philip Mudd says, initially curious, over time people become increasingly interested; they might be desensitised to the harms of terrorism and might decide to join the struggle. Individual terrorists known as lone wolves receive information from the Internet about how to kill people in the most efficient ways [54]. If behaviour is the product of a person-situation interaction, then attempting to change behavior by addressing the situation is an important endeavor [55], [56]. The goal of situation intervention is to inhibit unwanted behaviour in specific contexts. Opportunity reduction involves manipulating the immediate environmental contingencies to increase the perceived costs of engaging in terrorism. A reduction in opportunities can hinder activities and may deter those individuals less determined to take part in violence.

Internet service providers (ISPs) have a central role to play in opportunity reduction, though their legal obligations vary across jurisdictions. Much of what ISPs can do in this regard depends on self-regulation and the extent of their cooperation with security agencies. All major ISPs have codes of conduct. Codes of conduct should ensure that Internet content complies with and service provider act in accordance with the laws and principles of social responsibility. These codes should meet community concerns and industry needs, operating as an accountability system that guarantees a high level of credibility and quality. Because of the transnational nature of Internet communications, coordinated activity among Internet intermediaries in different jurisdictions is an essential element of self-regulation. Also needed is the widespread use of rating and filtering technology. To this end, content providers should be mobilized to label their content voluntarily, and filters must be made available to empower Netusers to make effective choices about the information they receive. Jurisdictions that endorse intermediaries' self-regulation should measure the effectiveness of such regulatory mechanisms to determine what national and transnational measures—if any—are necessary to compensate for the intermediaries' deficiencies [57].

Large ISPs should have active cyber patrols that search for violent content. They also should have integrity teams that are authorized to require providers to remove inappropriate content. For example, internal mechanisms should be in place to prohibit the images of beheadings, the glorification of terrorist acts, and the incitement to murder [58]. Because they know that the Internet has been used for radicalizing individuals and recruiting terrorists, Internet intermediaries should be proactive in averting acts of terror.

Large ISPs also should have easily identifiable and easily accessible hotlines to enable Netusers to report illegal activities. Most certainly, ISPs should not be conduits for illegal and antisocial activities. Take YouTube as an example. For a number of years, YouTube has provided an important platform for terrorist propaganda. Dozens of videos on the site provide guidance to terrorists [59]. Half of all terrorist videos contain explicit deadly violence. The effects of exposure to this violence are profoundly negative [60]. Ostensibly, YouTube has what it calls "Respect the YouTube" community standards [61]. One of these standards, which pertains to violent and graphic content, states:

> It's not okay to post violent or gory content that's primarily intended to be shocking, sensational, or disrespectful. If posting graphic content in a news or documentary context, please be mindful to provide enough information to help people understand what's going on in the video. Don't encourage others to commit specific acts of violence [61].

YouTube, however, is not adequately enforcing its own standards. Having community standards and not enforcing them is a sham.

More than just a video-hosting site, YouTube also is a formidable social networking forum. Contributors can draw the attention of registered subscribers who then are able to comment on video uploads and communicate with the source. Users are able to subscribe to each other's feeds based on mutual interests. This channel of communication attracted the interest of the Pakistani Taliban to spread propaganda, engage in dialogue with viewers, and recruit persons interested in joining a foreign terrorist organization [62].

In March 2019, a terrorist murdered 49 people and wounded 48 others in shootings at two mosques in Christchurch, New Zealand. This was the nation's deadliest attack. The terrorist livestreamed the rampage at Al Noor mosque to Facebook from a head-mounted camera. The livestream of the attack lasted for 17 minutes. Through social media, the terrorist conveyed his racist, hateful, and violent messages that quickly found their way onto the front pages of some of the world's largest news websites in the form of still images, GIF images (i.e., a series of images or silent video that loops continuously and does not require the viewer to press or click "play"), and full video with images and sound [63], [64]. One version of the Christchurch video was left live on Facebook for at least six hours, while others were available on YouTube for at least three hours [65]. The footage was viewed more than 4,000 times before it was removed [66]. It took 29 minutes to detect the livestreamed video, which is eight minutes longer than it took police to arrest the terrorist. About 1.3 million copies of the video were blocked from Facebook, though 300,000 copies had been published and shared [67]. Facebook spokesman Simon Dilner said that the company could have done a better job and was prepared for regulatory action. Several companies, including ANZ bank in Australia and ASB bank in New Zealand, stopped advertising on Facebook after Facebook was widely condemned by the public [67]. Under pressure to mend its ways, in May 2019 Facebook announced it was tightening rules around its livestreaming feature. The announcement came ahead of a meeting of world leaders aimed at curbing online violence in the

aftermath of the massacre in New Zealand [68]. French President Emmanuel Macron has said he wants to introduce new rules that would punish any site that publishes violent content or extreme opinions [69].

Internet intermediaries, however, argue that human review of all uploaded videos before they become publicly available is impossible. The volume, they say, is far too large, and the technology not sufficiently advanced to promptly flag such events. Such a stance overlooks the real problem. The problem is not one of *ability* but of *will*. For any abuse of technology there is a technological answer. Internet intermediaries should focus their attention on improvements to machine learning in concert with human oversight. It is not beyond their reach to devise algorithms that would flag shooting sounds and words such as *shoot*, *kill*, and *murder* in tandem. Footages that contain these sounds and words would immediately come to the attention of moderators who would then decide whether to act and block the footage.

After the Christchurch terror attack, Facebook announced that it would be investing in research to build better technology to quickly identify edited versions of violent videos and images and prevent people from resharing these altered versions [70]. Calls to include significant time delays for livestreams are impractical, as the result might be detrimental to the legitimate livestreaming of many good causes critical to the public interest.

Internet intermediaries should closely monitor violent terroristic forums and issue alerts to warn Netusers and readers of problematic content. I recommend the use of two other tools: registration and Stop! messages.

3.1 Registration Requirement

In many research libraries, books known to be problematic for their content are kept in designated areas under the open eye of an experienced librarian. If someone wants to read a book from that section, that person must sign for it and read it in the same room where the book is kept. This procedure enables the library to balance the right to free expression and the availability of information with societal interests in maintaining peace and order. People who have library cards still have access to the information, though they might be asked questions about why they want to read the book and a record kept that they have read the book in question. Similar arrangements can be made on the Internet. Problematic material would have restricted access. People would be required to sign up to read the material and provide details about their identity and why they want to read the material. If someone wants to read a manual on how to kill people, for example, the prospective reader would need to leave verifiable details about identity and purpose. Similarly, if someone is interested in accessing recipes for making bombs, that person would need to accept some interference with personal privacy. We should not be neutral about this kind of content. Morally speaking and in keeping with CSR, we cannot be neutral regarding such alarming speech. At the very least, this kind of speech requires some precautionary measures. These precautions would promote a greater level of trust in the technology. A balance needs to be struck between freedom of expression and social responsibility.

3.2. Stop! Messages

Stop! messages would be designed to pop up whenever someone tries to access dangerous, terroristic information. The following is an example of a Stop! message:

Stop!
You are about to access information of a terroristic nature that is dangerous. No information about your IP address will be stored when this page is displayed. The purpose of this message is to prevent dissemination of antisocial and violent information. If you want to forward tips to the police about terrorism or terrorists, please click on the link here.

Such warning messages would arouse the conscience of users about the harmful nature of terrorism. These messages aim to reduce the permissibility of violence speech. Furthermore, such messages would increase the level of perceived risk in the minds of potential jihadists and terrorists. Although users would attempt to remain anonymous, these kinds of messages may prompt suspicion in the minds of users that perhaps they are being watched by security agencies. Stop! messages also could warn users about the potential for psychological harm from viewing the material and provide advice on where to go for help.

Various Internet intermediaries publicize bomb recipes. Manuals on making terror devices, including nail bombs and the chemical agent ricin, have been found to be openly available on YouTube and Facebook [71]. Context, of course, is important. Such recipes on terror sites amount to incitement. Philip Mudd, associate executive assistant director of the FBI, has said that there will not be laws banning the posting of such recipes because Americans perceive the matter as a free-speech issue [52]. Mudd contends that people should be allowed to post this information because doing so is not a crime. He concedes, however, that planting bombs is a crime [52]. Still, an Internet provider may decide there is no room for such information on its server. Similarly, providers may choose to not allow terrorist propaganda on their servers. Providers may ask themselves: Why should I carry this? Self-policing is fine. According to Mudd, government interference instructing what is legitimate and what is not legitimate is objectionable [52].

Undoubtedly, some of the bombs used in terrorist acts were inspired by the Internet. The criminals took the recipes from the Internet. In September 2017, U.K. Prime Minister Theresa May urged Google and Facebook to stop do-it-yourself bomb-making manuals from appearing online after a crude homemade device exploded on the Parsons Green tube [72]. Twenty-nine people were injured in that terror attack. Still, the United States is willing to pay this price—even though that worldview affects not only the United States but also many other countries.[6]

4. Government Regulation

The major Internet intermediaries are, for the time being, American. The intermediaries see the Internet as a free highway for the exchange of opinions and for making money. They are products of the First Amendment and the "land of the free." These companies have been enjoying much freedom.

[6] It should be noted that federal law in the United States prohibits the distribution of bomb-making instructions. See subsection 842(p) of title 18 of the United States Code. At the same time, in the balancing act between free speech and national security, much evidence is required to make such speech illegal. See Doyle, C. (2003, September 10). *Bomb-making online: An abridged sketch of federal criminal law* [Congressional Research Service report for Congress]. Damascus, MD: Penny Hill Press. Retrieved from https://fas.org/sgp/crs/misc/RS21616.pdf

In historical terms, the Internet is an infant. It came into our lives between 1993 and 1994; thus, it is less than 30 years old. The Western world has been slow to devise ways to fight Internet abuse and has left much responsibility for curbing abuses to the Internet giants. They have failed to deliver a safe and secure environment and continue to permit much abuse.

In 2018, the Intelligence and Security Committee of the British Parliament published its report on the 2017 terror attacks.[7] Because many of these terrorist attacks had an online element, the committee concluded that Internet intermediaries have a responsibility to notify the authorities when they find terrorism online and to allow the authorities to take preventive action. While some Internet companies attributed their lack of monitoring to the need to protect users' privacy, this argument should not be allowed to prevail when there is concrete danger to human life [73]. Failure to alert the authorities in a timely fashion prevents early detection of potential threats [73]. The committee voiced its disappointment that little progress has been made in tackling terrorism online despite government pleadings and calls for action [73].[8]

The Christchurch, New Zealand, terrorist cited a white-genocide conspiracy theory as the main justification for the terror attack. That conspiracy theory was circulated on several Facebook pages. For many years, Facebook has allowed extreme groups that endorse violence, including Nazi groups and white supremacists, to use the company's platform to proliferate their views and facilitate communication among members because its business model is to enable the widest possible freedom of expression. Facebook's data for 2018 show that it removed 12.4 million pieces of "terrorist content" in six months and that around 2.5 million pieces of hate speech were deleted during the first quarter of that year [74]. The two main questions are: (1) Why were these pieces of information allowed on Facebook in the first place? and (2) How many pieces of such information are still propagating hate and violence on Facebook?

In March 2019, in light of an international outcry protesting Facebook's irresponsible conduct, the giant company announced that it intended to change its policy and would block "praise, support and representation of white nationalism and separatism" [75]. Facebook also pledged to improve its ability to identify and block material from terrorist groups. In the past, Facebook had allowed white-nationalist content on its server, as it did not deem these messages to be racist; instead, the company believed the messages were on a par with "things like American pride and Basque separatism, which are an important part of people's identity" [75]. Thus, Facebook believed that calls to create white ethno-states or claims that the United States should be a "white only" nation were protected speech under the First Amendment [76]. Facebook ignored the context of when and where these statements were made, which generally

---

[7] On March 22, 2017, Khalid Masood drove a hired car across Westminster Bridge, killing four pedestrians and injuring dozens more. He then ran into Parliament Square and fatally stabbed police officer Keith Palmer. On May 22, 2017, suicide bomber Salman Abedi detonated a homemade device in the lobby of Manchester Arena at the end of an Ariana Grande concert. This was the deadliest terror attack on British soil since the July 7 bombings in London in 2005. Twenty-two people were killed, and more than 200 people were injured. On June 3, 2017, three terrorists drove a van into pedestrians on London Bridge. Eight people were killed in the attack. On June 19, 2017, a terrorist drove a van into a group of Muslim worshippers outside Finsbury Park Mosque. He killed one person and injured several others. On September 15, 2017, an improvised explosive device was detonated on a packed tube train during the morning rush hour, injuring 22 people.

[8] For further discussion, see *Government Response to the Intelligence and security Committee of Parliament Report "The 2017 Attacks: What needs to change?"* (2019, January). [Report No. CP 22]. London, England: APS Group. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/778895/CCS207_CCS0119361008-001_Gov_response_2017_Attacks_Accessible.pdf

carried the suggestion that followers should be prepared to use force against non-whites. What Facebook apparently overlooked, however, were the likely implications of such speech when the speakers are known figures in the violent white-supremacist movement. Facebook regarded many such statements as mere advocacy when they really amounted to incitement, which is unprotected speech even in the United States. Speech cannot be judged independently, irrespective of the identity of the speaker, the speaker's intentions, the speaker's audience, and the circumstances under which the words were spoken. Capitalist urges to make money, however, serve as huge incentives to publish almost without limitation. The Internet intermediaries' business model prescribes making profit as the guiding rule. Companies make money when they publish, not when they censor. Atrocious terror events that resulted in dozens of casualties—including a racist attack on a black church in Charleston, South Carolina, in 2015; a car attack on protesters in Charlottesville, Virginia, in 2017; a mass shooting at a synagogue in Pittsburgh, Pennsylvania, in 2018; and a terror attack on two mosques in Christchurch, New Zealand, in 2019—prompted Facebook to reconsider its position, realizing that white nationalism could not be "meaningfully separated" from white supremacy and organized hate groups [75]. To detect more content relating to real-world harm, Facebook is updating its artificial intelligence (AI) to better catch first-person shooting videos and is working with American and British law enforcement officials to obtain camera footage from their firearms training programs to help its AI team learn what real, first-person violent events look like [77].

The production and distribution of media for foreign terrorist organizations constitutes material support for terrorism. Service providers that knowingly assist in the distribution of terrorist media are also culpable. Internet intermediaries must be made to realize that they can neither turn a blind eye to the use of their services by terrorist organizations nor continue to put the onus of identifying and removing terrorist media on private citizens [60]. While I find it hard to believe that Google, operator of YouTube, has an interest in promoting terrorism, and while Google has taken some steps to address the danger emanating from YouTube and other digital platforms, Google can and should do more. Because Google and other companies are reluctant to take the necessary steps, it is the role of governments to step in and demand a far more efficient proactive fight against online terrorism.

In a series of articles, I have sounded alerts about Internet abuse and called for change [78]-[84]. Change, however, is very slow. It is now clear to me that self-regulation does not work. The Internet and its major companies that earn billions of dollars from online activities need to be regulated. Otherwise, the abuse will continue, and many more people will lose their lives on the altar of freedom of expression. It is time for change. Liberal democracy has an obligation to protect vulnerable parties. Governments must step in to ensure that terrorism and other evils on the Internet do not enjoy freedom to harm.

On March 30, 2019, Facebook Chairman and Chief Executive Officer Mark Zuckerberg surprised many people (me included) by saying that there was a need for governments and regulators to have "a more active role" in four areas: harmful content, election integrity, privacy, and data portability. Zuckerberg maintained:

> Every day we make decisions about what speech is harmful, what constitutes political advertising, and how to prevent sophisticated cyberattacks... These are important for keeping our community safe.

> But if we were starting from scratch, we wouldn't ask companies to make these judgments alone [85].

Zuckerberg said that legislation was important for "protecting elections" and expressed his belief that

> we need a more active role for governments and regulators. By updating the rules for the Internet, we can preserve what's best about it—the freedom for people to express themselves and for entrepreneurs to build new things—while also protecting society from broader harms [85].

I was less surprised to read a few weeks later that Facebook also sent another message to Washington: Don't take Zuckerberg's suggestion too seriously. In a flurry of calls and emails to regulators, consumer groups, and think tanks, Facebook operatives explained that Zuckerberg was not encouraging new limits on speech in the United States. His target was mostly overseas regulators, the operatives said, and noted that Zuckerberg had other ideas for Washington [86]. Facebook tries to navigate a fraught political terrain and to seek a workable formula for different countries, in accordance with their different social norms and legal provisions.

Former U.K. Attorney General (2010-2014) and former chair of the Intelligence and Security Committee of Parliament (2017-2019) Dominic Grieve has said he supports regulation of the Internet to ensure that it does not serve and promote terrorism and other antisocial and criminal conduct [87]. British Culture Secretary Jeremy Wright announced in May 2019: "The era of self-regulation for online companies is over. . . . Voluntary actions from industry to tackle online harms have not been applied consistently or gone far enough" [88]. Also, in May 2019, Home Secretary Sajid Javid said that despite repeated calls to action, harmful and illegal content is still too readily available online. Therefore, he added, the British government has decided to force Internet intermediaries to clean up their act once and for all [88].

On April 8, 2019, the U.K. Department for Digital, Culture, Media & Sport and the Home Office published a white paper about online harms. The paper endorsed a requirement for proactivity on the part of Internet intermediaries, forcing the intermediaries to ensure that they have effective and proportionate processes and governance in place to reduce the risk of illegal and harmful activity on their platforms and to take appropriate and proportionate action when issues arise. According to the paper, the new regulations would ensure effective oversight of the take-down of illegal content and introduce specific monitoring requirements for tightly defined categories of illegal content [17]. The paper also suggested the establishment of a new regulatory framework for online safety that would make companies tackle harm caused by content or activity on their services. The regulatory body, according to the paper, would have the power to take effective enforcement action against companies that breached their statutory duty of care. Enforcement actions could include, for example, the levying of substantial fines and the imposition of liability on individual members of senior management. The regulatory body also would have the power to require the submission of additional information about alleged violations (including information about the impact of algorithms used to select content for users) and to ensure that companies proactively report emerging and known harms. The paper calls for companies to invest

in the development of safety technologies to reduce the burden on users who want to stay safe online [17].

In his comments on a draft of the white paper, Jack Goldstone said that as long as a platform acts as a media company in any way (e.g., accepts advertising, sells information about users, presents material from providers that are represented as news for their audiences), then the platform should be subject to the same laws on content as all other major media companies, such as television networks or news magazines. The printing press and the television were hailed in their early days as the great vanguard for free and open communication, just like the Internet is today; therefore, if the two older media have been regulated for the good of society, why not regulate the Internet?

5. CleaNet

Once data are available in digital form, questions arise about who can disseminate the data, who owns the data, who provides access to the data, who may have access to the data (including restrictions to access), and who may use the data. It is time to consider the introduction of a new browser funded by an affluent person with a sense of social responsibility, a nongovernmental organization (NGO), or a group of NGOs that wants to establish a better Internet future for our children (such as The Deliberative Democracy Consortium, or DDC).[9] The DDC, vowing that it will have no connections to any government, has stepped forward and taken on the task of developing a new browser called CleaNet. Being cognizant of potential governmental tendencies to restrict out-of-favor political speech under the pretence of "dangerous" and "terrorist" speech, no government will be involved in this delicate, deliberative process.

Deliberative democracy directly involves citizens in the decision-making process on matters of public concern. It requires the establishment of public institutions through which knowledge is exchanged and ideas crystallized through deliberation and critical reflection. Democratic procedures establish a network of pragmatic considerations and a constant flow of relevant information. People present their cases in persuasive ways, trying to bring others to accept their proposals. Deliberation takes place through the exchange of information among the parties who introduce and critically test proposals. Deliberations are free of any coercion, and all parties are substantially and formally equal—in terms of standing, ability, and opportunity to table proposals, offer compromises, suggest solutions, and support some motions and criticize others. Each participant has an equal voice in the process and tries to find reasons that are persuasive to all in order to promote the common good [89], [90]. Because the Internet affects the life of each and every one of us, we have a vested interest in attempting to have a social tool that enables the promotion of the social good. Following Jürgen Habermas' ideas on deliberative democracy and the importance of having access to different publics and organizations in the international civil society, it is argued that the Internet will be stable in the long run only if Netusers generally perceive it as a legitimate instrument and only

[9] The Deliberative Democracy Consortium (DDC) is a collaborative network of practitioners and researchers from more than 50 organizations and universities that seeks to strengthen the field of deliberative democracy. The DDC supports research activities and aims to advance practice at all levels of government around the world. For more information about the DDC, see http://www.deliberative-democracy.net/

if the Internet is perceived as right and good based on shared values and norms [31], [90]-[93].[10]

The first step in developing CleaNet will be to create a decision-making framework. It is proposed that the CleaNet framework consist of five components arranged in a hierarchical structure: Select Committee, International Steering Committee, Netcitizens Committee, a Complaints Committee, and a Hotline (see Figure 1).

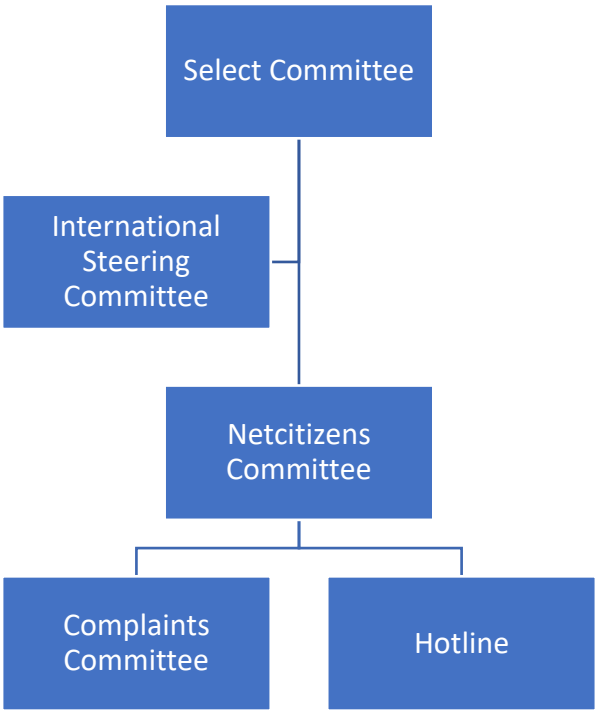

Figure 1. CleaNet framework for decision-making

With the framework in place, the next step will be to appoint a Select Committee whose members will be nominated by the owners of the new browser. NGOs representing new media, human rights organizations, freedom-of-expression societies, and institutions that promote social responsibility will be invited to serve on the Select Committee.

An International Steering Committee of national representatives will be formed to learn from each other's experiences, cooperate in case of need, exchange views, and deliberate sensitive issues. As Habermas explained, such public discourse filters reasons and information, topics and contributions in a way that the discourse outcome enjoys a presumption of rational acceptability [90]. At the same time, according to Habermas, the public discourse establishes relations of mutual understanding that are "violence-free," in

[10] For further discussion, see van Dijk, J. A. G. M., & Hacker, K. L. (2018). *Internet and democracy in the network society*. London, England: Routledge.

the sense that participants seek uncoerced agreement rather than domination or manipulation of others. Habermas described the forms of communication that constitute political discourse as structures of mutual recognition [90].

Next, a Netcitizens Committee will be convened. It would decide what should be excluded from the new browser and which problematic topics should be regarded as unprotected speech. A public open call for Netcitizens Committee members will be issued, and the process will be conducted with transparency, full disclosure, and open deliberation and debate. Clear deadlines for each step of the process will be outlined to ensure that the process will not linger for many months. Members of the Netcitizens Committee will be chosen by the Select Committee. The aim will be to include representatives of ISPs, web-hosting companies; Internet experts; media professionals; Internet scholars; government officials; human-rights and minority-rights organizations; freedom-of-speech organizations; computer engineers; judges and lawyers; and other interested parties. This representation is of crucial importance, as minorities frequently face difficulty in having an equal voice and equal standing in decision-making processes.

The Netcitizens Committee will include no fewer than 100 people and no more than 400 people, depending on the number of applicants willing to commit themselves for the responsible work at hand. The committee needs to be a working committee. It cannot be too large.

In some respects, the structure of the CleaNet's organization will resemble that of the Internet Corporation for Assigned Names and Numbers (ICANN) model. ICANN is a private-sector, nonprofit, global corporation with multiple stakeholders. The organization is responsible for IP-address space allocation, protocol-parameter assignment, domain-name system management, and root-server system management functions [94]. ICANN's global stakeholders include companies that offer domain names to the public; companies that operate top-level domain registries; ISPs; intellectual-property interests; business users; noncommercial users (such as academics, NGOs, nonprofit organizations, consumer advocates, individual Internet users, and governments) [94]. ICANN has four advisory committees that provide advice and recommendations. These committees represent governments and international treaty organizations, root-server operators, persons concerned with Internet security, and the general community (i.e., average Internet users). ICANN also has a Technical Liaison Group that works with organizations responsible for devising the basic protocols for Internet technologies [95]. As of mid-2013, the ICANN Governmental Advisory Committee represented 125 nations (plus the African Union Commission, the European Union, and the Vatican). ICANN's Country Code Names Supporting Organization represents more than 135 country-code domains, while its At-Large Advisory Committee includes more than 150 representatives from all geographic regions [94].[11]

The CleaNet Netcitizens Committee members will commit to working for one year, renewable for two more years, at most. After one year, the least active members will be asked to leave, and they will be replaced by others. It is expected that a third of the

[11] For further discussion, see Goldsmith, J., & Wu, T. (2006). *Who controls the Internet? Illusions of a borderless world*. New York, NY: Oxford University Press; Pohle, J., & Morganti, L. (2012). The Internet Corporation for Assigned Names and Numbers (ICANN): Origins, stakes and tensions. *Revue française d'études américaines*, *4*(134), 29-46; and Zittrain, J. (2014, March 24). No, Barack Obama isn't handing control of the Internet over to China. *The New Republic*. Retrieved from https://newrepublic.com/article/117093/us-withdraws-icann-why-its-no-big-deal

committee will change each year. Such a reshuffle is advisable and productive. It keeps the committee energetic, engaged, viable, and fresh with ideas.

Because the work is hard and demanding, with considerable societal implications, members of the Netcitizens Committee will be paid for their work. The payment should not be too meagre nor should it be very substantial. It should be enough to provide an incentive, given the responsible work at stake, but it should not be the main job of the committee's members. It is recommended that the payment be between 1,000 and 2,000 euros per month.

The first issue on the agenda will be to determine what speech should be ousted from the Internet. The next issue will be to specify the parameters for identifying problematic, antisocial speech. The committee will consider the wide needs and interests of the public in an open, transparent, and critical way. All committee members will have the opportunity to participate and voice an opinion, present arguments, submit criticisms and reservations, and respond to counterarguments. No one will ever be excluded from the deliberative process. The committee will try to reach a consensus in delineating the scope of legitimate and acceptable Internet speech. In the absence of a consensus, decisions may be made by voting; however, the committee needs to make every effort to reach a consensual decision that reflects widespread public needs and interests. The broadest possible consensus would ensure the legitimacy of the committee's decisions. Because the committee represents Western-liberal tradition, the scope of legitimate and acceptable speech should be as wide as possible. Whenever it comes to restrictions on speech, the onus for limiting free expression always is on the person who wants to limit expression. Concrete evidence always should be provided to justify any restrictions on expression. For speech to be restricted, it must be dangerous and/or harmful. The danger and/or harm cannot be implicit or implied. If speech were to be prohibited only because its danger might be implied from an unclear purpose that is opened to interpretation, then the scope for curtailing fundamental democratic rights is too broad, and the slippery-slope syndrome becomes tangible. The implicit way is not the path that liberals should tread when pondering restrictions on freedom of expression.

Throughout the CleaNet development process, each participant will be able to exercise "communicative freedoms," a term that Habermas applied to activities that seek to achieve mutual understanding through reasoned discourse [90]. Such open, deliberative discourse allows everyone to participate in the processes of opinion- and will-formation in which individuals exercise their autonomy [90]. When the list of requirements for excluded speech has been completed, the list will be given to software engineers to design the algorithm for detecting material that should be banned from the new browser.

In a sense, CleaNet will be an enhanced, citizen-based form of server filtering. A detailed Terms of Fair Conduct will be drafted. Only material that is deemed problematic and affirmed by at least 80% of the members on the Netcitizens Committee will be listed for exclusion. A separate under-review list will comprise debatable speech that needs to be considered and debated periodically until a resolution to either allow or filter the material has been achieved. The under-review list also will include problematic material that is allowed on CleaNet but is accessible to only those Netusers who sign up to access the content. It will be the responsibility of the ISPs and web-hosting companies to retain a list of Netusers who access the restricted content and to cooperate with law-enforcement whenever needed. After the list of requirements for exclusion of content has been completed, the list will be given to software engineers who then will design an algorithm to detect material that should be removed from CleaNet.

CleaNet will be launched during a special news conference to let the public know that the new browser is available for use, explain the rationale for developing a new browser, and explain the significance of the browser's ability to detect and exclude dangerous content. The news conference will stress that CleaNet can be downloaded for free and may be used by anyone. After downloading CleaNet, Netusers will have two options: (1) keep the browser(s) they have been using but add CleaNet as an alternative (primary or secondary) browser, or (2) replace their current browser(s) with CleaNet.

CleaNet will be attentive to societal cultural norms. For example, while Holocaust denial is not problematic in the United States, it is particularly problematic in Germany and Israel. The CleaNet will pay special attention to such sensitive matters.

It is assumed that while international consensus has been reached about excluding certain antisocial material (i.e., child pornography, cyberbullying, and the promotion of violent crime and terrorism) from CleaNet, such a consensus cannot be expected for content related to hate and bigotry. The notable exception to this lack of consensus will likely be the United States. Such tolerant norms, however, are not universal. It is not reasonable to expect other countries to believe that the Internet should be free of bigotry and hatred. CleaNet users therefore can opt to filter such material.

After CleaNet has been implemented and is widely available in the marketplace, government officials in each country will need to promote and encourage the use of CleaNet in the public sector. Only governmental agencies that have a specific interest in studying antisocial material should be granted permission to use other browsers. The assumption is that the public sector has no need for access to, for example, child pornography, criminal speech, terrorism, and bigotry.

On CleaNet, search engines will not keep their ranking-algorithms secret. Quite the opposite. They will proudly announce that the ordering of search results is influenced by standards of moral and social responsibility, commitment to preserving and promoting security online and offline, and adherence to liberal principles we hold dear: liberty, tolerance, human dignity, respect for others, and not harming others.

The assumption is that once people become aware of the advantages of CleaNet, they will prefer it over the browsers they had been using. Ongoing open discussions about the merits of and the flow of information on the new browser are expected. Attempts will be made to remedy any problems with the flow of information.

The entire process of debating, implementing, and browsing with CleaNet will be transparent and open for criticism and feedback. Netcitizens will be welcomed to provide criticism on the CleaNet hotline and will receive an answer within 24 hours. Netcitizens will have the option of making their feedback public or keeping it private, with or without attribution in either case.

Paid CleaNet officers will screen the hotline comments and pass thought-provoking complaints to a Complaints Committee. The Complaints Committee will be a subcommittee of the Netcitizens Committee and will include 20 to 40 members. Subcommittee members will receive an additional compensation of 500 to 1,000 euros for their work. It is assumed that members will consider it a great honor and privilege to sit on the Complaints Committee and therefore would see no reason for a higher salary despite the hard work involved. The Complaints Committee will study the complaints it receives and will issue a reasoned response within a month.

By the end of each year, the Netcitizens Committee and the Complaints Committee will issue an annual report about their work, which will be freely available to all interested parties and posted on the CleaNet website. The reports will be as detailed as possible and include the terms of practice and how those terms were implemented;

reflections on the year's work; lessons learned; the reasoning behind specific decisions; and recommendations for the future.

The hotline will be operated by a team of paid professionals who will provide an effective and speedy response to all questions and criticisms. The hotline will provide easy accessibility to Internet users and an assured response. Queries and answers will be transparent. They will be posted on the hotline website. Transparency also means that the rules and procedures for addressing users' concerns will be explained at the point of entry. The CleaNet rationale will be explained in detail, and additional help will be made available if needed. Netusers will be able to track their concern throughout the submission and review processes and will be informed of the final outcome. The Netcitizens Committee will make available to the public annual reports of the basic statistics.

One may ask: How is CleaNet different from any of the multiple commercial products that offer filtering of Internet and web-based content? To start with, CleaNet will be the result of democratic and open deliberations involving citizens. The decision-making process will involve concerned citizens who will decide together what the future Internet should look like. They will be involved in an ongoing process, offering reasoning and counter-reasoning where everything will be put on the table for discussion. Furthermore, CleaNet will be more comprehensive than any existing filter. Whereas some filters are designed to help parents ensure that their children will not encounter pornography on the Internet (e.g., NetNanny.com) and others are designed to filter hate (e.g., HateFilter.com [96]), CleaNet will be a transparent browser that will provide Netusers with the ability to surf the Internet in a social, friendly environment, free of the antisocial, evil material that is now so prevalent and accessible on existing browsers.[12] In addition, CleaNet will be a pragmatic, deliberative, democratic, fluid tool that is sensitive to cultural norms and open to contestation. It will be designed by the people and for the people to address people's needs and concerns. CleaNet has been suggested precisely because no existing filter can achieve the desired outcome of a clean Internet with full transparency about relevant considerations for permitting and not permitting certain content and citizens' ability to deliberate, exchange ideas, and influence cyber surfing.

6. Conclusion

The Internet has obvious advantages for modern terrorism. The Internet is diffused and decentralized and lacks a coherent structure. It is also global and quite chaotic. The threat of terrorism is real and significant. As the Internet became a major arena for modern terrorists, we need to devise appropriate methods to forestall their activities and establish security. To tackle abuse of the Internet by terrorists, governments developed a crisis-response mechanism that involves the establishment of networks of "online first responders" within technology companies. These first responders are directly linked to the heart of international governments' counterterrorism units and law enforcement

[12] For more information, see Cohen-Almagor, R. (2018, May). Addressing Internet dangerous expressions: Deliberative democracy and CleaNet. *Journal of Internet Law*, *21*(11), 3-15. I first proposed the idea of CleaNet in my book, *Confronting the Internet's Dark Side: Moral and Social Responsibility on the Free Highway*, explaining in detail the rationale for its establishment.

agencies, an arrangement that facilitates rapid and coordinated responses aimed at stopping the spread of violent extremist content [97].

The Internet is ubiquitous, interactive, fast, and decentralized. The ease of access to the Internet along with its low cost, rapid speed, user (individuals and groups) anonymity, and the international character provide all kinds of individuals and organizations an easy and effective arena for spreading their partisan interests. The Internet contains some of the best products of humanity and some of the worst. It simultaneously serves the positive and negative elements in society.

Increasingly, the relationships among hate speech, hate crime, and acts of terror are becoming very clear. We need to balance two important principles: freedom of expression and social responsibility. The forefathers of the Internet had the vision of creating a free highway, a public space where everyone can say what they want. This wonderful innovation of a wholly unfettered platform has backfired. The Internet is open for use and abuse. We should provide and promote responsible use while at the same time fight against those who abuse the Internet. The challenges are on all levels: individual, community, state, and international. We are in the early stages of learning how to cope with and combat the abuse. Slowly, we are developing the necessary tools to enjoy innovation and freedom while at the same time adopting safeguards and rules of responsible conduct.

The success of such efforts depends not only on how we use the Internet but also how well the Internet gatekeepers act as responsible filters of content. These companies possess immense power. Power without responsibility is dangerous. Power without responsibility is corrosive. Power without responsibility undermines our well-being. Therefore, we must insist that Internet intermediaries take responsibility and ensure that Netusers can enjoy the vast capabilities of the Internet without putting themselves in danger. The Internet's way should not be in harm's way. The Internet's way should be enlightening, innovative, entertaining, productive, and the voice of the best of humanity. To achieve this vision of the Internet, boundaries should be introduced, antisocial and violent activities should be curbed, and a safe environment should be established through the combined efforts of Netusers, businesses, countries, and the international community at large.

More than 25 years after the Internet entered its mass commercial phase, we can now conclude that self-regulation does not work. Self-regulation does not work for offline media [98], [99], and it certainly is failing online. Governments must step in and enforce cohesive and protective rules of conduct to prevent harm, protect vulnerable populations, and save lives. Now that we have learned the hard way the consequences of having a powerful free highway of technology, it is time for change.

References

[1] Martin, G. (2014). *Essentials of terrorism*. Thousand Oaks, CA: SAGE.

[2] Martin, G. (2013). *Understanding terrorism*. Thousand Oaks, CA: SAGE.

[3] Matusitz, J. (2013). *Terrorism and communication*. Thousand Oaks, CA: SAGE.

[4] Weimann, G. (2013). *Terror on the Internet: The new arena, the new challenges*. Washington, DC: U.S. Institute of Peace Press.

[5] Cohen-Almagor, R. (2017, November). The role of Internet intermediaries in tackling terrorism online. *Fordham Law Review*, *86*(2), 425-453.

[6] Council of Europe Committee on Counter-Terrorism. (2017, December 9). *Extract from CM (2017)131-add (pgs 53-55)*. Strasbourg, France: Council of Europe Committee on Counter-Terrorism.

[7] Skrzypek, J. K. (2013). *Is terrorism theatre? Dramaturgical metaphor in the cases of Budyonnovsk, Dubrovka and Beslan* (Unpublished doctoral dissertation). University of St. Andrews, St Andrews, Fife, Scotland.
[8] McDonald, K. (2018). *Radicalization*. Cambridge, England: Polity Press.
[9] Malashenko, A., Bowers, S. R., & Ciobanu, V. (2001). *Encyclopedia of jihad*. Harrisonburg, VA: William R. Nelson Institute.
[10] Jihad, In BBC archive. Retrieved from http://www.bbc.co.uk/religion/religions/islam/beliefs/jihad_1.shtml
[11] Mutahhari, M. (n.d.). *Jihad: The holy war of Islam and its legitimacy in the Quran* (M. S. Tawhidi, Trans.). Ahlul Bayt Digital Islamic Library Project. Retrieved from http://www.al-islam.org/short/jihad/
[12] Bunt, G. R. (2003). *Islam in the digital age*. London, England: Pluto Press.
[13] Goodpaster, K. E. (2010). Corporate responsibility and its constituents. In Brenkert, G. G., & Beauchamp, T. L. (Eds.), *The Oxford handbook of business ethics* (pp. 126-157). New York, NY: Oxford University Press.
[14] Abend, G. (2014). *The moral background: An inquiry into the history of business ethics*. Princeton, NJ: Princeton University Press.
[15] Kerr, M., Janda, R., & Pitts, C. (2009). *Corporate social responsibility: A legal analysis*. Markham, Ontario: LexisNexis.
[16] Weissbrodt, D. (2010). Untitled review of the book *Social responsibility: A legal analysis*, by Michael Kerr, Richard Janda, Chip Pitts]. *Human Rights Quarterly*, *32*(1), 207-215.
[17] Secretary of State for Digital, Culture, Media & Sport and the Secretary of State for the Home Department. (2019, April). *Online harms white paper* (Paper CP 57, presented to the Parliament of the United Kingdom). London, England: Home Office.
[18] Carroll, A. B. (1979). A three-dimensional conceptual model of corporate social performance. *Academy of Management Review*, *4*(4), 497-505.
[19] Carroll, A. B. (1981). *Business and society: Managing corporate social performance*. Boston, MA: Little, Brown.
[20] Crane, A., Matten, D., McWilliams, A., Moon, J., & Siegel, D. S. (Eds.). (2009, September). *The Oxford handbook of corporate social responsibility*. New York, NY: Oxford Handbooks Online.
[21] Carroll, A. B. (1999, September). Corporate social responsibility. *Business & Society*, *38*(3), 268-295.
[22] Carroll, A. B., & Buchholtz, A. K. (2011). *Business and society: Ethics and stakeholder management*. New York, NY: South-Western College.
[23] Tarabasz, A. (2019). Corporate social responsibility in times of Internet (in)security. In A. Bartoli, J.-L. Guerrero, & P. Hermel (Eds.), *Responsible organizations in the global context* (pp. 237-250). London, England: Palgrave.
[24] Kraakman, R. H. (1986, Spring). Gatekeepers: The anatomy of a third-party enforcement strategy. *Journal of Law, Economics, & Organization*, *2*(1), 53-104.
[25] Cohen-Almagor, R. (2015). Netcitizenship: Addressing cyberevenge and sexbullying. Journal of Applied Ethics and Philosophy, 7, 14-23.
[26] Habermas, J. (1990). *Between facts and norms*. Cambridge, England: Polity Press.
[27] Habermas, J. (1990). *Moral consciousness and communicative action*. Cambridge, MA: MIT Press.
[28] Macedo, S. (1999). *Deliberative politics: Essays on democracy and disagreement*. New York, NY: Oxford University Press.
[29] Gutmann, A., & Thompson, D. F. (2004). *Why deliberative democracy?* Princeton, NJ: Princeton University Press.
[30] Dryzek, J. S. (2002). *Deliberative democracy and beyond*. Oxford, England: Oxford University Press.
[31] Dryzek, J. S. (2012). *Foundations and frontiers of deliberative governance*. New York, NY: Oxford University Press.
[32] Bächtiger, A., Dryzek, J. S., Mansbridge, J., & Warren, M. (Eds.). (2018). *The Oxford handbook of deliberative democracy*. Oxford, England: Oxford University Press.
[33] Sageman, M. (2004). *Understanding terror networks*. Philadelphia, PA: University of Pennsylvania Press.
[34] Robinson, G. E. (2020). *Global jihad*. Stanford, CA: Stanford University Press.
[35] Beech, H., & Gutierrez, J. (2019, March 24). An ISIS couple's troubling path to terror recruiting. *The New York Times*. Retrieved from https://www.nytimes.com/2019/03/24/world/asia/isis-philippines-syria.html?emc=edit_th_190324&nl=todaysheadlines&nlid=338024680324
[36] Cohen-Almagor, R. (2017). Jihad online: How do terrorists use the Internet? In F. C. Freire, X. R. Araújo, V. A. M. Fernández, & X. L. García (Eds.), *Media and metamedia management* (pp. 55-66). Dordrecht, Netherlands: Springer.
[37] Rocha, I. M. & Mendoza, H. T. (Eds.). (2020). *Jihadism, foreign fighters and radicalization in the EU: Legal, functional and psychosocial responses*. London, England: Routledge.

[38] *Jihadist use of social media—How to prevent terrorism and preserve innovation: Hearing before the Subcommittee on Counterterrorism and Intelligence, of the House Committee on Homeland Security*, 112th Cong. 13 (2011) (testimony of Brian Michael Jenkins, Senior Advisor to the President, RAND).
[39] *Internet terror recruitment and tradecraft—How can we address an evolving tool while protecting free speech?: Hearing before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, of the House Committee on Homeland Security*, 111th Cong. 14 (2010) (testimony of Brian Michael Jenkins, Senior Advisor to the President, RAND).
[40] Stalinsky, S. & Sosnow, R. (2020). *From Al-Qaeda to the Islamic State (ISIS), jihadi groups engage in cyber jihad: From 1980s promotion of use of "electronic technologies" to today's embrace of social media to attract a new jihadi generation*. Washington, DC: MEMRI.
[41] Interviews I conducted with Daniel Castro, Information Technology and Innovation Foundation, and with Brian Marcus, former Director of Internet Monitoring, Washington, DC (May 9, 2008 and June 5, 2008).
[42] Atwan, A. B. (2012). *The secret history of al-Qaeda*. London, England: Saqi Books.
[43] Forest, J. J. F. (2006). Preface. In J. J. F. Forest (Ed.), *Teaching terror: Strategic and tactical learning in the terrorist world* (p. xii). Lanham, MD: Rowman & Littlefield.
[44] Maruf, H. & Joseph, D. (2018). *Inside Al-Shabaab: The secret history of Al-Qaeda's most powerful ally*. Bloomington, IN: Indiana University Press.
[45] Matusitz, J. (2020). *Global jihad in Muslim and non-Muslim contexts*. London, England: Palgrave.
[46] General Intelligence and Security Service of the Netherlands (2012). *Jihadism on the web: A breeding ground for jihad in the modern age*. Ministry of the Interior and Kingdom Relations: The Hague, Netherlands. Retrieved from https://www.aivd.nl/onderwerpen/terrorisme/documenten/publicaties/2012/02/14/het-jihadistisch-internet-kraamkamer-van-de-hedendaagse-jihad
[47] Sageman, M. (2008). *Leaderless jihad: Terror networks in the twenty-first century*. Philadelphia, PA: University of Pennsylvania Press.
[48] JMG (Jihadi Monitory Group) Desk. (2012, March 3). *In the depths of jihadist web forums: Understanding a key component of the propaganda of jihad*. Herzliya, Israel: International Institute for Counter-Terrorism.
[49] Zelin, A. Y. (2008). *The state of global jihad online: A qualitative, quantitative, and cross-lingual analysis*. Washington, DC: New America Foundation.
[50] Qin, J., Zhou, Y., Reid, E., & Chen, H. (2008). Studying global extremist organizations' Internet presence using the dark web attribute system: A three region comparison study. In H. Chen, E. Reid, J. Sinai, A. Silke, & B. Ganor (Eds.), *Terrorism informatics* (pp. 237-266). New York, NY: Springer.
[51] Cohen-Almagor, R. (2015). *Confronting the Internet's dark side: Moral and social responsibility on the free highway*. New York, NY: Cambridge University Press.
[52] Interview with Philip Mudd, Associate Executive Assistant Director, National Security Branch, Federal Bureau of Investigation, Woodrow Wilson Center (March 25, 2008).
[53] Choi, K., Lee, C. S., & Cardigan, R. (2018). Spreading propaganda in cyberspace: Comparing cyber-resource usage of Al Qaeda and ISIS. *International Journal of Cybersecurity Intelligence and Cybercrime, 1*(1), 21-39.
[54] Netflix. (2018). *Terrorism close calls* [Streaming documentary series]. Retrieved from https://www.netflix.com/gb/title/80185048
[55] Smith, M. J. (2003). *Theory for practice in situational crime prevention*. Boulder, CO: Lynne Rienner.
[56] Wortley, R., & Mazerolle, L. (Eds.). (2013). *Environmental criminology and crime analysis*. London, England.
[57] Waltermann, J., & Machill, M. (Eds.). (2000). *Protecting our children on the Internet: Towards a new culture of responsibility*. Gütersloh, Germany: Bertelsmann Foundation.
[58] Meleagrou-Hitchens, A. (2020). *Incitement: Anwar al-Awlaki's western jihad*. Cambridge, MA: Harvard University Press.
[59] *Terror guides and bomb-making manuals "openly available on social media."* (2017, May 25). Sky News. Retrieved from https://news.sky.com/story/terror-guides-and-bomb-making-manuals-openly-available-on-social-media-10892201
[60] *Jihadist Use of Social Media—How to Prevent Terrorism and Preserve Innovation: Hearing before the Subcommittee on Counterterrorism and Intelligence, of the House Committee on Homeland Security*, 112th Cong. 8 (2011) (testimony of Andrew Aaron Weisburd, Director, Society for Internet Research).
[61] *Rules and policies: Community guidelines*. (n.d.). YouTube. Retrieved from http://www.youtube.com/yt/policyandsafety/communityguidelines.html
[62] *Jihadist Use of Social Media—How to Prevent Terrorism and Preserve Innovation: Hearing before the Subcommittee on Counterterrorism and Intelligence, of the House Committee on Homeland Security*, 112th Cong. 27 (2011) (testimony of Evan F. Kohlmann with Josh Lefkowitz and Laith Alkhouri).
[63] Wakefield, J. (2019, March 16). *Christchurch shootings: Social media races to stop attack footage*. BBC. Retrieved from https://www.bbc.co.uk/news/technology-47583393

[64] *Christchurch shootings: 49 dead in New Zealand mosque attacks*. (2019, March 15). BBC. Retrieved from https://www.bbc.co.uk/news/world-asia-47578798
[65] Martinson, J. (2019, March 24). Christchurch attacks: The media's rush to be first causes its own kind of harm. *The Guardian*. Retrieved from https://www.theguardian.com/media/commentisfree/2019/mar/24/christchurch-attacks-the-medias-rush-to-be-first-causes-its-own-kind-of-harm?utm_term=RWRpdG9yaWFsX0d1YXJkaWFuVG9kYXlVS19XZWVrZGF5cy0xOTAzMjU%3D&utm_source=esp&utm_medium=Email&utm_campaign=GuardianTodayUK&CMP=GTUK_email
[66] *Facebook to ban white nationalism and separatism*. (2019, March 28). BBC. Retrieved from https://www.bbc.co.uk/news/world-us-canada-47728471
[67] Anderson, C. (2019, March 24). Censor bans "manifesto" of Christchurch mosque shooter. *The Guardian*. Retrieved from https://www.theguardian.com/world/2019/mar/24/censor-bans-manifesto-of-christchurch-mosque-shooter?utm_term=RWRpdG9yaWFsX0d1YXJkaWFuVG9kYXlVS19XZWVrZW5kLTE5MDMyNA%3D%3D&utm_source=esp&utm_medium=Email&utm_campaign=GuardianTodayUK&CMP=GTUK_email
[68] Facebook restricts Live feature, citing New Zealand shooting. (2019, May 14). *Reuters*. Retrieved from https://www.reuters.com/article/facebook-extremists/facebook-restricts-live-feature-citing-new-zealand-shooting-idUSL5N22R05J
[69] Reid, D. (2019, May 14). *Big tech must take the lead against hate*. City A.M. Retrieved from http://www.cityam.com/277554/big-tech-must-take-lead-against-hate
[70] Wong, J. C. (2019, March 29). Facebook finally responds to New Zealand on Christchurch attack. *The Guardian*. Retrieved from https://www.theguardian.com/us-news/2019/mar/29/facebook-new-zealand-christchurch-attack-response?utm_term=RWRpdG9yaWFsX0d1YXJkaWFuVG9kYXlVS19XZWVrZW5kLTE5MDMzMA%3D%3D&utm_source=esp&utm_medium=Email&utm_campaign=GuardianTodayUK&CMP=GTUK_email
[71] Mostrous, A. (2017, May 25). Facebook and YouTube publish DIY terror guides on how to make bombs. *The Times*. Retrieved from https://www.thetimes.co.uk/article/facebook-and-youtube-publish-diy-terror-guides-on-how-to-make-bombs-2h00mr5px
[72] Harper, P. (2017, September 16). Theresa May orders Google, Facebook and YouTube to stop bomb manuals appearing online after "crude" DIY explosive is detonated at Parsons Green. *The Sun*. Retrieved from https://www.thesun.co.uk/news/4477628/theresa-may-orders-google-facebook-and-youtube-to-stop-bomb-manuals-appearing-online-after-crude-diy-explosive-is-detonated-at-parsons-green/
[73] Intelligence and Security Committee of Parliament. (2018, November 22). *The 2017 Attacks: What needs to change?* [Report No. HC 1694]. London, England: APS Group. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/776162/HC1694_The2017Attacks_WhatNeedsToChange.pdf
[74] Dearden, L. (2019, March 25). Neo-Nazi groups allowed to stay on Facebook because they "do not violate community standards." *The Independent*. Retrieved from https://www.independent.co.uk/news/uk/home-news/facebook-new-zealand-neo-nazis-white-supremacists-a8837886.html
[75] *Facebook to ban white nationalism and separatism*. (2019, March 28). BBC. Retrieved from https://www.bbc.co.uk/news/world-us-canada-47728471
[76] Beckett, L. (2019, March 27). Facebook to ban white nationalism and separatism content. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2019/mar/27/facebook-white-nationalism-hate-speech-ban
[77] *Facebook expands definition of terrorist organizations to limit extremism*. (2019, September 17). Slashdot. Retrieved from https://tech.slashdot.org/story/19/09/17/2229247/facebook-expands-definition-of-terrorist-organizations-to-limit-extremism
[78] Cohen-Almagor, R. (2018). Taking North American white supremacist groups seriously: The scope and the challenge of hate speech on the Internet. *International Journal of Crime, Justice, and Social Democracy*, *7*(2), 38-57.
[79] Cohen-Almagor, R. (2018, March-April). Social responsibility on the Internet: Addressing the challenge of cyberbullying. *Aggression and Violent Behavior*, *39*, 42-52.
[80] Cohen-Almagor, R. (2017). Balancing Freedom of Expression and Social Responsibility on the Internet. *Philosophia*, *45*(3), 973-985.
[81] Cohen-Almagor, R. (2013, May). Online child sex offenders: Challenges and counter-measures. *Howard Journal of Criminal Justice*, *52*(2), 190-215.
[82] Cohen-Almagor, R. (2012). In Internet's way: Radical, terrorist Islamists on the free highway. *International Journal of Cyber Warfare and Terrorism*, *2*(3), 39-58.
[83] Cohen-Almagor, R. (2012). Freedom of expression, Internet responsibility and business ethics: The Yahoo! saga and its aftermath. *Journal of Business Ethics*, *106*(3), 353-365.
[84] Cohen-Almagor, R. (2011). Fighting hate and bigotry on the Internet. *Policy and Internet*, *3*(3), 1-26.

[85] Mark Zuckerberg calls for stronger regulation of Internet. (2019, March 30). *The Guardian*. Retrieved from https://www.theguardian.com/technology/2019/mar/30/mark-zuckerberg-calls-for-stronger-regulation-of-internet?utm_term=RWRpdG9yaWFsX0d1YXJkaWFuVG9kYXlVS19XZWVrZGF5cy0xOTA0MDE%3D&utm_source=esp&utm_medium=Email&utm_campaign=GuardianTodayUK&CMP=GTUK_email
[86] Kang, C. (2019, April 21). It's U.S vs. world as big tech faces specter of limiting speech online. *The New York Times*. Retrieved from https://www.nytimes.com/2019/04/21/technology/facebook-zuckerberg-harmful-speech.html?emc=edit_th_190422&nl=todaysheadlines&nlid=338024680422
[87] Author's meeting with Dominic Grieve MP, British Parliament (April 4, 2019).
[88] Duncan, C. (2019, April 7). Social media firms including Facebook and Twitter to be legally forced to protect users. *The Independent*. Retrieved from https://www.independent.co.uk/news/uk/politics/social-media-regulation-facebook-twitter-government-jeremy-wright-a8858981.html
[89] Cohen, J. (1989). Deliberation and democratic legitimacy. In A. Hamlin & P. Petit (Eds.), *The good polity* (pp. 22-23). Oxford, England: Blackwell.
[90] Habermas, J. (1998). *Between facts and norms: Contributions to a discourse theory of law and democracy* (W. Rehg, Trans.). Cambridge, MA: MIT Press.
[91] Habermas, J. (1990). *Moral consciousness and communicative action* (C. Lenhardt & S. W. Nicholsen, Trans.). Cambridge, MA: MIT Press.
[92] Fishkin, J. S. (1993). *Democracy and deliberation*. New Haven, CT: Yale University Press.
[93] Chappell, Z. (2012). *Deliberative democracy*. Houndmills, England: Palgrave Macmillan.
[94] *A quick look at ICANN: The Internet Corporation for Assigned Names and Numbers* [Pamphlet]. (n.d.). n.p.: ICANN. Retrieved from https://www.icann.org/en/system/files/files/quick-look-icann-01nov13-en.pdf
[95] *What does ICANN do?* (n.d.). n.p.: Internet Corporation for Assigned Names and Numbers. Retrieved from https://www.icann.org/resources/pages/what-2012-02-25-en
[96] Seminerio, M. (1998, November 11). *ADL launches "HateFilter" to combat racist sites*. ZDNet. Retrieved from http://www.zdnet.com/article/adl-launches-hatefilter-to-combat-racist-sites/.
[97] Woodcock, A. (2019, June 27). Facebook and YouTube must do more to stop terrorists live streaming atrocities, May to tell G20. *The Independent*. Retrieved from https://www.independent.co.uk/news/uk/politics/theresa-may-facebook-youtube-terrorists-live-streaming-g20-a8977846.html
[98] Cohen-Almagor, R. (2005). *Speech, media, and ethics: The limits of free expression*. Houndmills, England: Palgrave Macmillan.
[99] Cohen-Almagor, R. (2014, April). After Leveson: Recommendations for instituting the public and press council. *International Journal of Press/Politics*, *19*(2), 202-225.