EUROPEAN JOURNAL OF GEOPOLITICS
vol. 9, 2021

Jakub SZYDELSKI
Warsaw Univ., Warsaw, Poland

TERRORISTS' ACTIVITIES ON-LINE DURING COVID-19 PANDEMIC - THE EUROPEAN PERSPECCTIVE

Abstract:

This essay presents the overview of the terrorists' activities online during the CoViD-19 pandemic. It points out the key trends in cyber-security and terrorism threat in 2020 and 2021 . These trends are illustrated with major violent incidents and cyber-attacks. Research focuses mainly on the European perspective. EU agencies' reports are frequently cited and the Europol findings are often referred to. During 2020 terrorists used various online platforms. These included Dark Web markets, hidden discussion groups, as well as social media platforms like TikTok. Global lockdown and health crisis affected online propaganda. This research focuses on the narrative of jihadists, far-right activists and the conspiracy theories believers. The impact of CoViD-19 pandemic on extremist propaganda is examined. European states' democratic institutions were vulnerable due to CoViD-19 pandemic. There were major cyber-attacks on the European states' local and central governments. The attacks on the German and American legislature are discussed and compared. The key finding is the terrorists' usage of online platforms and apps during 2020. Dark Web was used primarily for logistics. Social media and hidden discussion groups were employed for sharing propaganda and disinformation. Encrypted communicators were used for confident chat. This essay does not exhaust the topic of terrorists' activities, it rather serves as a general overview. Still more data is needed to assess full threat level of online terrorism.

Key words:
CoViD-19, terrorism, on-line media, conspiracy theories, jihadists, EU

Szydelski, J. (2021). Terrorists' activities on-line during CoViD-19 pandemic – the European perspective, *European Journal of Geopolitics*, 9, pp. 19-35.

INTRODUCTION

Due to CoViD-19 global pandemic the Internet usage in Europe increased[1]. National lockdowns introduced by many European states changed the ways people communicate, meet and work on-line.

There were notable terrorism attacks in 2020 and at the beginning of 2021. Europe was struggling with Hanau shootings in February (Germany) and the Vienna shooting in November (Austria). The United States were shaken by the attack on the Capitol Building on 6th of January 2021.

At the time of writing this essay (January 2021) there was not enough data to compare the scale of terrorist attacks in 2019 and 2020. All major international reports covering this topics are updated annually. This is the case of the Global Terrorism Database (GTD), as well as the European Union Terrorism Situation and Trend report (TE-SAT), to name a few.

Considering the above, I decided to address the issue of terrorists' Internet activity during the CoViD-19 pandemic. My goal was to outline a few of the key trends in daily operation of terrorist organizations nowadays. I focused mainly on the European perspective.

DEFINITION, METHODOLOGY & SOURCES

Terrorism has been described by many definitions, but European Union did not create their own. Instead, the European Commission agreed on the definition provided by the International Organization for Migration (IOM) in its publication "Glossary on Migration".

IOM defines **terrorism** as "intentional and systematic use of actions designed to provoke terror in the public as a means to certain ends. (…)"[2]. This definition also states, that only "civil population" could be treated as terrorism victims.

It is also worth adding, that cyberterrorism is beyond the main scope of this research. Elizabeth Minei & Jonathan

[1] Statista. https://www.statista.com/statistics/1110864/online-media-use-during-the-coronavirus-pandemic-europe/
[2] European Commission. https://ec.europa.eu/home-affairs/e-library/glossary/terrorism_en

Szydelski, J. (2021). Terrorists' activities on-line during CoViD-19 pandemic – the European perspective, *European Journal of Geopolitics*, 9, pp. 19-35.

Matusitz (2012) define **cyberterrorism** as "a method of attack designed to damage, tamper with, or destroy critical points of national infrastructure by controlling and manipulating computer networks".

Following these definitions I focused on the online activities of terrorist organizations, mainly propaganda, communication and recruitment.

During my research I relied heavily on the Europol statistics. Official Europol reports were covering the problem of organized crime from the European perspective, what corresponded with the topic of this essay.

Selected reports of EU agencies' offered valuable insight into terrorism and cybersecurity. I referred to the research of ENISA, which is European Union Agency for Cybersecurity. The other useful source was CT MORSE, which is EU project on counter-terrorism (CT).

Other sources consisted of respected European scientific institutes and think-tanks. Among these were: Fondation pour la recherche stratégique (FRS), Istituto per gli Studi di Politica Internazionale (ISPI), The Global Network on Extremism and Technology (GNET).

Only few sources had non-European heritage, mainly the UNITAR documents, but I opted not to exclude these reports, as they presented high professional level.

TARGET GROUPS

With nearly 90% of European citizens being active online,[3] the terrorist groups are likely to exploit social media for their propaganda as well as recruitment. It is therefore appropriate to point out distinct social groups, that could be targeted.

These target groups were mostly derived from publication by Gary Ackerman and Hayley Paterson (2020). Authors defined key impacts of COVID-19 pandemic on terrorism.

First of all, **conspiracy theories believers**. They are likely to be attracted by an original content. Such materials

[3] European Union Internet Users, Population and Facebook Statistics. https://www.internetworldstats.com/stats9.htm

Szydelski, J. (2021). Terrorists' activities on-line during CoViD-19 pandemic – the European perspective, *European Journal of Geopolitics*, 9, pp. 19-35.

may support their beliefs, such as the "Coronavirus hoax". These groups typically follow alternative media channels (e.g. QAnon). They are more susceptible to extremists propaganda and may react accordingly to the hostile narrative encouraging violence.

Secondly, **far-right and far-left sympathizers/activists**. CoViD-19 pandemic may have resulted in radicalization of European citizens. Ackerman and Paterson are describing situations of scapegoating the "others" for the virus. These actions fuel strong anti-immigrant resentment.

Thirdly, **anti-government protesters**. They could be connected with the previous group, but it is not always the case. Hard lockdowns imposed in many countries raised levels of frustration among the population. Mishandling of the health crisis by the state bodies in many cases resulted in social unrests (Henley 2020).

Fourthly**, victims of epidemic**. It could be any European, who suffered a loss of a loved one, or is currently facing financial problems. Global recession and lockdowns affected millions and many could feel sense of injustice. With limited access to the critical opinion of other people, the isolated internet users may become more susceptible to propaganda and conspiracy theories.

INFODEMIC

As governments were trying to flatten the epidemic curve, there was second obstacle emerging. "Information pandemic" or "Infodemic" is believed to represent the current negative trend. Term was further popularized by the Secretary-General of the United Nations when he mentioned it in his tweet from March 2020.[4]

Infodemic is a "blend of "information" and "epidemic" that typically refers to a rapid and far-reaching spread of both accurate and inaccurate information"[5]. During crisis situation news channels could be "flooded" by rumours, as well as

[4] Twitter. https://twitter.com/antonioguterres/status/1243748397019992065
[5] Merrian Webster. https://www.merriam-webster.com/words-at-play/words-were-watching-infodemic-meaning

disinformation, what makes it difficult to gain proper knowledge on current affairs.

Before May 2020 Europol[6] noted an increase in online propaganda materials. Simultaneously there was growing number of conspiracy theories online. The prediction is that due to unstable and polarized media climate more and more extremists would be pushed to their ideological fringes. This in turn may result in spiral of radicalization in 2021.

DARK WEB USAGE BY TERRORISTS

Dark Web (or Darknet) is the part of the internet, "that is encrypted and that cannot be found using ordinary search engines"[7]. It could be used for criminal activity, notably for trade in illegal goods and services. These goods could vary from drugs, to fake passports and firearms.

Dark Web is associated with anonymity, as most of its users protect their sensitive data, such as IP addresses. This could be achieved through VPN (Virtual Private Network) or TOR System. Both tools enable its users to hide or mask their original IP address. During the pandemic usage of these systems increased. Accordingly, Tor Project Inc. adjusted its marketing strategy and created up-to-date slogan: "Resist the surveillance pandemic".

Throughout the 2020 there was an increase in Dark Web business trade, according to latest Europol report on the Internet organized crime.[8] The surge was observed in multiple areas. The most important change, related to terrorism, could be the shift from the legitimate-looking counterfeit passports to "registered" e-passports" as well as e-IDs. Such documents might allow easier access to transportation and accommodation in foreign countries and could be used by point man, liaison officer or even suicide bomber. Fake IDs

[6] Europol. How CoViD-19-related crime infected Europe during 2020. https://www.europol.europa.eu/publications-documents/how-covid-19-related-crime-infected-europe-during-2020
[7] Cambridge Dictionary. https://dictionary.cambridge.org/dictionary/english/dark-web
[8] Europol. Internet organised crime threat assessment 2020. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

Szydelski, J. (2021). Terrorists' activities on-line during CoViD-19 pandemic – the European perspective, *European Journal of Geopolitics*, 9, pp. 19-35.

enable terrorists to create safe bank accounts, as the real owner remains in the shadow.

Dark Market was called the world's largest Dark Web marketplace. It was used by nearly 500 000 online customers and facilitated over 320 000 transactions. Vendors traded in illegal products like drugs, anonymous SIM cards and malware. Dark Market site was taken offline by the Europol on 12th of January 2021[9]. Officers seized the servers located in Moldova and Ukraine. German police arrested an Australian who was the alleged operator of the site.

Europol officers also took part in the takedown of the hosting service used by the criminals.[10] Investigation showed, that three domains – INSORG.ORG; SAFE-INET.COM and SAFE-INET.NET. – offered "bullet proof hosting services"[11]. This involved concealing true identity of cybercriminals responsible for ransomware, E-skimming breaches (infecting checkout pages), phishing (stealing user data by infected mail) and account takeovers.

Shutdowns of illegal Darknet sites are essential for online safety. Equally important is constant tracking of Dark Web market. Analysing illegal business trade helps to predict means of potential terrorist attacks, including cyberattacks on critical infrastructure. On the other hand Darknet could not be as easily used for determining terrorists targets. Ghadah Alrasheed & Brandon Rigato argue (2019), that modern terrorists are not using Dark Web for communication and propaganda. The primary reason is limited reach in comparison to Twitter of Facebook.

ONLINE JIHADIST PROPAGANDA

With the downfall of Deash in 2017 its primary agitation platform – Al Hayat Media – went silent in the main stream. Nevertheless the jihadist propaganda prevails in social media.

[9] Europol. https://www.europol.europa.eu/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down
[10] Europol. https://www.europol.europa.eu/newsroom/news/cybercriminals%E2%80%99-favourite-vpn-taken-down-in-global-action
[11] US Department of Justice. https://www.justice.gov/usao-edmi/pr/us-law-enforcement-joins-international-partners-disrupt-vpn-service-used-facilitate

Cyber jihadists are still exceptionally active on Instagram and Twitter. Jihadist movement didn't confine itself to well-established, main channels of communication. They were also experimenting with the relatively new social media app – TikTok. In October 2019 the Wall Street Journal informed about the videos produced by the Islamic State supporters. Footage depicted corpses, as well as fighters with guns. Chinese media outlet decided to remove accounts responsible for ISIS propaganda (Taylor 2020).

Despite TikTok intervention, extremists still use the applications for radicalization and propaganda. Throughout September 2020 a Pakistani imam, Luqman Haider, posted videos praising Charlie Hebdo attacker. Before becoming influencer he taught Qur'anic lessons to kids and teenagers.

Jihadists are targeting youth with appropriate channels. They are constantly adapting new social media apps, as they are following the trends. Apart from TikTok IS fighters were using video game forums and dating apps.

Dr. Hugo Micheron (2020) implies, that Jihadists succeeded in reaching to young audience. Chechen, who beheaded Samuel Paty in front of high school was 18 years old. Vienna attacker, who shot four people and wounded twenty three was only two years older.

Jihadists used multiple narrations concerning pandemic. One of the most well-known was "COVID-19 as God's 'smallest soldier". Pierre Boussel (2020) observes, that the message could be "God sends a message for the faithful". It could be retribution on the rich countries, because lockdowns affected mostly their economy. Likewise COVID-19 could be seen as a punishment to world leaders, who fought against ISIS.

ON-LINE RECRUITMENT OF JIHADISTS

One of the key impacts of CoViD-19 pandemic may have been increased recruitment online. It was listed as one the key negative trends in the UNITAR report for 2020.[12]

[12] UNITAR. Impact of COVID-19 on violent Extremism and terrorism. https://unitar.org/learning-solutions/publications/impact-covid-19-violent-extremism-and-terrorism

The ground-breaking study of Anne Speckhard and Molly Ellenberg (2020) demonstrates a vast potential of online recruitment. The study concentrated on foreign terrorist fighters of ISIS Caliphate in Syria and Iraq. Out of 236 fighters, 49% of men and 52.6% of women were recruited digitally. During the recruitment candidates were contacted online by ISIS recruiter.

Even more surprisingly, 17.7% (42 people) departed for Syria only after watching propaganda online. Other mean of communication was messaging local facilitator. What is important, is that a face-to-face meeting was not necessary.

Interviewees of this study included many ISIS fighters, who came from Europe. They were of many nationalities – Irish, British, Swiss, Dutch. This study shows great extent to which European citizens are susceptible to terrorism recruitment online.

Although the research of Anne Speckhard and Molly Ellenberg was conducted in 2015 – 2019 timeframe, it still points out the global trend. Present excessive use of internet communicators and social media could have only intensified this process.

USE OF AN ENCRYPTED COMUNICATION BY TERRORISTS

End-to-end encryption communication (E2EE) is thought as one of the safest and most secure way of contacting online. Messaging apps like WhatsApp, Signal and Telegram classify chat content. Sender app encrypts the message. Only the receiver app can decipher it. As third parties don't have access to the recipient decryption key, they can't spy on the conversation.

Encrypted communication has been employed by the terrorists in the past. It ensured, that their schemes remained confidential, as law enforcement agencies were unable to break messaging security system.

Encrypted messaging was used by many prominent ISIS fighters, including Abdelhamid Abaaoud, who orchestrated November 2015 terrorist attacks in Paris (Kean, Hamilton

2018). He used True Crypt for hard drive encryption, as well as communicators like Telegram and WhatsApp.

So far there was no evidence of encrypted messaging apps usage before the Vienna terrorist attack in November, or other terrorist attacks, that took place in Europe during 2020. Nevertheless European Commission pointed to the problem of encrypted information in its update[13] of Counter-Terrorism Agenda in December. It proposed financial investigations to help follow the money trail and identify those involved.

Update comes around the same time of the European Council's resolution on encryption.[14] Council stresses the need of lawful access to digital evidence of encrypted communicators. Decryption platform is now under construction, which will enable Europol officers to access encrypted information on devices, that were seized during investigation.

Recent changes in EU strategy have been criticized by some journalist and human rights activists on the basis of users' privacy concerns. EDRi (European Digital Rights association) observes[15], that there are better ways to decipher message without breaking the encryption system. EDRi states, that this method poses potential threat of excessive state surveillance.

CONSPIRACY THEORISTS RADICALIZATION

Three of the main disinformation factions during CoViD-19 pandemic were 5G oppositionists, QAnon supporters and anti-vaccination activists. Although many supporters of the conspiracy theories limit their actions to online activity and demonstration, radicalization of their views could lead to violent actions.

In 2019 researchers from Sydney analysed online activities of the right-wing extremists (Waldek, Ballsun-

[13] European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2326
[14] European Commission. First Progress Report on the EU Security Union Strategy. https://ec.europa.eu/info/sites/info/files/communication_on_the_first_progress_report_on_the_eu_security_union_strategy.pdf
[15] EDRi. Keep private communications private. https://edri.org/our-work/keep-private-communications-private/

Stanton, Droogan 2020). Study showed, that radicals were using two main communication channels. The first one was official Internet media, such as Facebook and Twitter. The second one – more hidden discussion groups like Gab, 4chan and 8chan.

These two channels differed in extremist narrative. Official accounts on Twitter echoed well-known theme of "white identity under threat". Racism could be fully expressed at the non-official forums. Researchers observed, that such platforms could perpetrate acts of terrorism and broadcast them to wider audience.

QAnon supporters widely used similar two channel communication, as the first posts were published on the "hidden" website 8chan around 2017 by anonymous author Q. Since 2017 he has instructed his followers via encrypted messages known as "Q drops".

Q claimed to be a high-ranked government official in the Trump administration. User stated, that he had a "Q" clearance. This means he would work at the US Department of Energy[16] and had access to the Top Secret Restricted Data.

QAnon groups and websites were originally visible in the Google search engine. Users created private group chats for every country, that was to be "endangered". In this way two basic communication channels were integrated. Facebook group could be start of a "rabbit hole". From there one could access other materials posted on websites like QNN.

Two channel communication was possible until Google, Facebook and Twitter banned groups and individual accounts[17]. This move possibly made QAnon fans move back to underground, where they are more difficult to monitor.

Current pandemic brought together conspiracy theorists and people of radical political views (Buranyi 2020). Protests against lockdowns and "Plandemic" are taking place in Europe's capitals such as London, Paris and Berlin. Q signs are widely seen among protesters, what confirms spread of the movement to Europe (Kesvani 2020).

[16] USGS, https://www.usgs.gov/about/organization/science-support/human-capital/national-security-code-designations-security
[17] Twitter. https://twitter.com/TwitterSafety/status/1285726278868402177

Europol analysts observed[18] increase in extremist propaganda published online in 2020. They argue, that online radicalization accelerated due to CoViD-19 pandemic. The first reason is quick adjustment of far-right and far-left agenda to the pandemic lockdowns and regulations. The second reason is greater exposition to radical propaganda, as Europeans tend to browse the Internet longer.

ANTI-5G MOVEMENT

Anti-5G activists finds life-threatening danger in operation of 5G radio infrastructure. The movement dates back to the introduction of the 5G mobile network in 2019. Since then there have been many protests against this system.

In 2020 demonstrations took place in many European countries like the UK, Germany and Spain. Anti 5G slogans often accompany demonstrations against CoViD-19 restrictions.

Although most QAnon supporters are far-right minded, the same cannot be said about anti-5G activists. Europol states, that ideological affiliation of this group is uncertain, although it has a link with anti-lockdown protesters.

Anti-5G activists methods resemble actions of anarchists or leftist militias, as they attack the property, not people (Loadenthal 2020). Main, typical targets of leftist militias are: government and police property, private businesses and telecommunication infrastructure. Method of violence – arson attack – is widespread among the anarchists, as they tend to incite cellphone masts.

During 2020 there were widespread arson attacks on 5G infrastructure. Out of 27 EU countries 10 were affected. As for 19th of October 2020 there were 183 mast attacks in Europe, according to the data gathered by online journal Politico.[19] Nearly 50% of incidents affected United Kingdom (87 out of 183).

[18] Europol, How COVID-19-related crime infected Europe during 2020, https://www.europol.europa.eu/publications-documents/how-covid-19-related-crime-infected-europe-during-2020

[19] Politico. Cerulus L. (2020). EU countries sound alarm about growing anti-5G movement.

In response to these incidents 15 EU member states called on the European Commission to counter-react anti-5G conspiracy theories.

CYBERATTACKS ON THE EUROPEAN STATES

Democratic institutions were under constant threat during CoViD-19 pandemic. Government administration was one of the most cyberattack-targeted sectors, according to ENISA report[20] on cybersecurity.

There were multiple cyberattacks on European states institutions throughout 2020. In Finland[21] and Norway[22] parliaments' computer systems were breached. As a result email accounts of MPs were compromised. Police is investigating this case as hacking and espionage.

French city Évreux suffered hacking into the municipal servers in December (Philippot 2020). Couple days earlier similar attack affected town hall of Braunau in Austria (Zeko 2020). Both attacks paralyzed the municipalities for several days.

Both local and central authorities were vulnerable to cyberattacks. What is more, the public health service was targeted. Attacks on medical service during health crisis fall in line with terrorism definition, as these actions would certainly provoke terror and chaos in the public.

Especially disturbing were the cyberattacks against the hospitals, which fought on the front-line of epidemic. On the 13th of March the University Hospital of Brno (Czech Republic) suffered major ransomware attack.[23] Malware encrypted the

[20] ENISA, Main incidents in the EU and worldwide, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents

[21] Euronews. (2020). Cyber attack in Finland hits email accounts of MPs and parliament https://www.euronews.com/2020/12/28/cyber-attack-in-finland-hits-email-accounts-of-mps-and-parliament

[22] Euronews. (2020). Norway's Intelligence Service says Russian groups 'likely' behind Parliament cyber attack. https://www.euronews.com/2020/12/08/norway-s-intelligence-service-says-russian-groups-likely-behind-parliament-cyber-attack

[23] Cyber Law Toolkit.https://cyberlaw.ccdcoe.org/wiki/Brno_University_Hospital_ransomware_attack_(2020)#cite_note-Porter-5

hospitals data. Staff was forced to shut down all the computers, as well as medical equipment linked to the IT network.

Other European states were also affected, primarily Germany, Italy and the UK. SAFECARE reported approximately 100 security incidents in the European hospitals from February to November.[24] 21 of them were cyber incidents. These included ransomware, phishing – sending fake mails impersonating the WHO and hijacking websites.

Hackers not only disturbed normal functioning of hospitals and laboratories, but also exposed sensitive data on patients. The Maze cybercriminal group demanded ransom from the research lab Hammersmith Medicines Research (HMR) (Schwartz 2020). When company didn't comply cybercriminals published private data of almost 2,300 patients. Materials included medical questionnaires and copies of passports or driving licenses.

ASSAULT ON DEMOCRATIC INSTITUTIONS

Apart from the cybercrime, European states had to cope with social unrest fueled by lockdown resentment. On 29th of August hundreds of far-right extremist tried to storm Reichstag[25] (German parliament building) during the demonstration against government restrictions. Offenders managed to reach the outside stairs before being pushed back by the police.

The attack on the Capitol Building is a striking example of alternative outcome. Hundreds of protesters broke into both chambers of Congress in session. Offenders vandalized offices of a few Congressmen (Brewster, Solender 2021). Trespassers were Donald Trump supporters, some were also conspiracy theory believers. Most of them exhibited presidential campaign gadgets like campaign flags and MAGA hats (Make America Great Again). Some of the participants wore QAnon shirts.

[24] SAFECARE. https://www.safecare-project.eu/?p=588
[25] The Guardian. (2020). 'Anti-corona' extremists try to storm German parliament. https://www.theguardian.com/world/2020/aug/29/berlin-braces-for-anti-coronavirus-protest-against-covid-19-restrictions

Events in the United States and Germany were alike in many ways. Firstly, they both occurred during mass demonstrations. Secondly, protesters were mostly affiliated with far-right movement. Thirdly, demonstrators assaulted the parliament building. This aspect is crucial. The legislature is the backbone of democratic governance. Attack on this institution and elected representatives is a brutal assault on the core of democratic system.

In the aftermath of the Capitol attack US Justice Department opened more than 25 domestic terrorism cases (Shalal, Shepardson 2021). Protesters actions could be considered as domestic terrorism, according to Congressional Research Service's Insight[26]. Trespassers could have intended to influence the policy of government by intimidation.

Events in United States and Europe prove, that every democratic system is vulnerable. Possible threats include terrorism, both domestic and foreign state-driven. Assault on Capitol should serve as a warning to European leaders of what could happen in Europe. Sometimes state's own citizens pose the greatest threat.

SUMMARY

Terrorists during CoViD-19 era focused mainly on propaganda distribution, logistics and recruitment. For propaganda they used two channel communication. They exploited official social media platforms, as well as alternative discussion groups. Logistics were handled via Dark Web markets. Recruitment and communication could have taken place via encrypted messaging apps like Signal or Telegram.

CoViD-19 pandemic resulted in more people being susceptible to online extremists narrative. Global crisis produced fertile ground for hostile propaganda and disinformation. In the current Infodemic environment such materials could lead to further radicalization and potentially harmful actions.

Attacks on the Bundestag and Capitol were the final effects of this radicalization process. The same could be said

[26] Congressional Research Service. https://crsreports.congress.gov/product/pdf/IN/IN11573

about the arson raids on 5G masts and terrorist attacks in Vienna. All these violent actions had roots in online media climate, reinforcing the feeling of injustice and the sense of danger.

European states were vulnerable to cyberterrorist attacks. Both local and central administration offices were targeted. Hackers managed to paralyze the work of state agencies and incited chaos. Especially worrying were the cyberattacks against the health service, as they could lead to patients' death.

Apart from the records on few terrorist attacks mentioned in this essay we still do not have enough data to assess the actual threat of terrorist online activities. In order to have a clear picture more studies are needed. Most valuable would be personal interviews with the internet users, as well as data mining analyses of the social media forums.

References

Ackerman, G., Peterson, H. (2020). *Terrorism and COVID-19: Actual and Potential Impacts. Perspectives on Terrorism*, https://www.universiteitleiden.nl/perspectives-on-terrorism/archives/2020#volume-xiv-issue-3

Alrasheed, G., Rigato, B. (2019). *Exploring the Dark Web: Where Terrorists Hide?* https://carleton.ca/align/2019/illuminate-exploring-the-dark-web-where-terrorists-hide/

Bousel, P. (2020). *Covid-19, jihadism and the challenge of a pandemic.* https://www.frstrategie.org/en/publications/notes/covid-19-jihadism-and-challenge-pandemic-2020

Brewster, J., Solender, A. (2021). *Clyburn's Ipad, Laptop From Pelosi's Office: Items Stolen, Destroyed In Capitol Attack.* Forbes.https://www.forbes.com/sites/jackbrewster/2021/01/08/clyburns-ipad-laptop-from-pelosis-office-items-stolen-destroyed-in-capitol-attack/?sh=49bd03fc5963

Buranyi, S. (2020). *How coronavirus has brought together conspiracy theorists and the far right.* BBC. https://www.theguardian.com/commentisfree/2020/sep/04/coronavirus-conspiracy-theorists-far-right-protests

Danielewicz, K. (2019). *Problem powrotu terrorystów z Państwa Islamskiego do Europy,* Przegląd Geopolityczny, 29, s. 53-66.

Fogaš, A., Verba, V. (2016). *Ongoing conflicts in the Middle East and their impact on Europe,* European Journal of Geopolitics, 4, pp. 51-67.

Henley, J. (2020). *Latest coronavirus lockdowns spark protests across Europe.* The Guardian.

https://www.theguardian.com/world/2020/nov/02/latest-coronavirus-lockdowns-spark-protests-across-europe
Kean, T.H., Hamilton, H.L. and others. (2018). *Digital Counterterrorism: Fighting Jihadists Online.* Bipartisan Policy Center. https://bipartisanpolicy.org/wpcontent/uploads/2019/03/BPC-National-Security-Digital-Counterterrorism.pdf
Kesvani, H. (2020). *QAnon Is No Longer Just America's Problem, It's Europe's Too.* Vice. Retrieved from https://www.vice.com/en/article/y3z8yk/qanon-conspiracy-theory-europe-spread-uk
Loadenthal, M. (2020). *The 2020 Pandemic and Its Effect on Anarchist Activity,* https://www.isponline.it/en/pubblicazione/2020-pandemic-and-its-effect-anarchist-activity-26157
Micheron, H., (2020). *Praising Jihadist Attacks on TikTok and the Challenge of Protecting Youths From Online Extremism*, https://gnet-research.org/2020/12/09/praising-jihadist-attacks-on-tiktok-and-the-challenge-of-protecting-youths-from-online-extremism/
Minei, E., Matusitz, J. (2012). *Cyberspace as a new arena for terroristic propaganda: an updated examination*, https://doi.org/10.1007/s10202-012-0108-3
Philippot, L. (2020). *Cyberattaque à Évreux : les services de la Ville et de l'agglomération paralysés*. France Bleu. https://www.francebleu.fr/infos/faits-divers-justice/cyberattaque-a-evreux-les-services-de-la-ville-et-de-l-agglomeration-paralyses-1608231627
Rogala-Lewicki, A. (2017). *Citizens' involvement in public sphere. Information as a ius publicum factor of the state of democracy*, European Journal of Geopolitics, 5, pp. 62-98.
Schwartz, S. (2020). *Report: Medical company set to aid coronavirus response struck by ransomware*. CIO Dive. https://www.ciodive.com/news/medical-company-coronavirus-ransomware/574653/
Shalal, A., Shepardson, D. (2021). *At least 25 domestic terrorism cases opened as result of assault on Capitol: lawmaker*. Reuters. https://www.reuters.com/article/us-usa-trump-capitol-cases/at-least-25-domestic-terrorism-cases-opened-as-result-of-assault-on-capitol-lawmaker-idUSKBN29F0NZ
Speckhard, A., Ellenberg, M. (2020). *Is Internet Recruitment Enough to Seduce a Vulnerable Individual into Terrorism?* Homeland Security Today. https://www.hstoday.us/subject-matter-areas/counterterrorism/is-internet-recruitment-enough-to-seduce-a-vulnerable-individual-into-terrorism/
Sykulski, L. (2019). *Diffused war as a kind of non-linear war*, Przegląd Geopolityczny, 29, s. 137-146.
Taylor, J. (2020). *Dangerous cures and viral hoaxes: Common coronavirus myths busted.* The Guardian. Retrieved from https://www.theguardian.com/media/2020/mar/28/dangerous-cures-and-viral-hoaxes-common-coronavirus-myths-busted

Waldek L., Ballsun-Stanton B., Droogan J. (2020), *Global Network, After Christchurch: Mapping Online Right-Wing Extremists*, https://gnet-research.org/2020/12/14/after-christchurch-mapping-online-right-wing-extremists/
Wasiuta, O., Wasiuta, S. (2018). *Asymmetric and hybrid geopolitical threats*, European Journal of Geopolitics, 6, pp. 4-36.
Wilczyński, P.L., Adamczyk, N., Matyja, M., 2020. *Prognoza konsekwencji kryzysu związanego z COVID-19 w opinii ekspertów*, Przegląd Geopolityczny, 34, s. 181-200.
Zeko, M., (2020). *Cyberattacke löst Chaos im Braunauer Rathaus aus.* Kronen Zeitung. https://www.krone.at/2289088