TRAMES, 2023, **27(77/72)**, 2, 115–126

DARK WEB − AS CHALLENGE OF THE CONTEMPORARY INFORMATION AGE

Nenad V. Denic and Sasa Devetak

University of Defense, Belgrade

Abstract. Reconnaissance and monitoring activities of actors on the Internet are becoming indispensable security tools for governments around the world. The Deep Web as part of the Internet protects actors. However, cheap and reliable encryption and online identity protection have become attractive to state and non-state actors in the cyber domain. Unfortunately, part of the Deep Web, the Dark Web is now offering to training terrorists, and trading arms and illicit substances. The Dark Web represents a communication and information systems infrastructure where actors are anonymous and the services are adaptable to the demands of geopolitical circumstances. This paper analyzes the ways of using the Dark Web and its impact on the information environment since the global war on terrorism began, through a period when humanity struggled with Covid-19 pandemic to the war in Ukraine.

Keywords: Deep Web, Dark Web, cyber, Covid-19, Russia, Ukraine

DOI: https://doi.org/10.3176/tr.2023.2.02

Received 26 February 2023, accepted 04 April 2023, printed and available online 20 June 2023

1. The Dark Web impact

Dark Web, a space on the Internet, is the logical structure mainly made to protect user identity and hide network activities. Following the 5D (*disinformation, deception, destabilization, disruption, and tailored destruction*) warfare era, the ability to hide the identity and intentions of actors in cyberspace are a supporting

© 2023 Authors. This is an Open Access article distributed under the terms and conditions of the Creative Commons Attribution 4.0 International License CC BY 4.0 (http://creativecommons.org/licenses/by/4.0).

asset, and Dark Web has become a powerful tool against state security. The Dark Web was a communication infrastructure for terrorist activities more than a decade ago. The network offered users complete identity hiding and high-quality, robust, and cheap encryption. Combining the network services with cryptocurrencies the Dark Web has been the space for indoctrination, recruitment, propaganda, and terrorist training. Covid-19 pandemic has pushed terrorism from the main information arena. Services of the Dark Web significantly influenced the information environment and became tools for propaganda, conspiracy theories, and selling medication for Covid-19 treatment. However, the Russian aggression against Ukraine has become a war with information. The operational environment of both sides has one more tool. It is the Dark Web, where both sides utilize services to their advantage. Therefore, the Dark Web has a significant impact on the global information environment. The Dark Web as the network for identity and activity protection in the cyber domain represents a global security risk during the war against terror, Covid-19 pandemic, and contemporary conflicts.

2. The online quest for safety and anonymity

The Internet, the network of all networks is supposed to provide all users with the same rights and possibilities. However, the Internet has to provide a certain level of security and anonymity for all users. The level of anonymity and security has shown a downward trend after the year 2000. States are increasingly exercising control over cyberspace to increase security in the physical domain. Average users of the Internet are searching for services using search engines. Internet search engines such as *Google, Bing, Yahoo, Baidu, Yandex,* and *Ask* are very useful tools in search for information. The popularity of the search engines depends on the region, but the use of the search engine also depends on the device used by users, for example, phones with the Android operating system use Google as the default search engine, while devices with the Microsoft operating system use the default, Bing. The most popular internet search engine in the world for all platforms (mobile phone, tablet, desktop laptop) from the data of internet site *Statcounter GlobalStats* is *Google* with a share of 92.20%, the second is *Bing* with 3.42% share (Statcounter Global Stats 2022). Internet search engines use an automatized process to gather as much data as possible on the Internet. Specialized software analyze databases made by indexed words for every document. When users search for a certain term, search engines use their algorithms to check the database and provide information about the term. The user generally receives information that depends on the algorithm of the internet search engine. Internet pages allow the previously mentioned specialized programs to collect data from them to make the page visible to as many users as possible. In most cases, website administrators optimize their pages so the search engines rank them in higher positions when the algorithm sends information to the user. In most cases, website administrators optimize their pages so that search engines rank them higher. The average Internet user thinks that the Internet is all that he can find using some internet search engines. However, the Internet is much larger than search

engines can index. The total percentage of indexed data on the Internet is estimated at 5% (60 Minutes CBS News 2015). The rest of the unindexed web pages is called the Deep Web, Hidden Web, or Invisible Web. The mentioned estimate of 5% is based on the total Internet traffic.

At the very beginning of the Internet, web pages were static and easy to index, but with the development of new technologies, things are becoming more and more complex. Dynamic web pages appear that cannot be indexed by conventional web browsers. A static website is linked to a single location on the Internet and the data on that page changes from time to time. On the other hand, dynamic internet pages are more complex and the only thing that is relatively constant is the page frame, while the data on the page depends on the data requested by the user. These pages are created based on user data requests and they are populated from related sources. Dynamic pages are becoming increasingly common, and therefore the unindexed part of the space between what is visible and what is invisible on the Internet has started to grow. The term Invisible Web was introduced in 1994. In that period, the term referred to information that was not visible to conventional Internet browsers (Bergman 2001).

The phrase Invisible Web was used until 2001 when Mihcael K. Bergman in his research paper "The deep web: Surfacing Hidden Value" introduced the new term Deep Web. An antonym of the Deep Web becomes Surface Web which was previously referred on Visible Web. The term Invisible Web only refers to web pages that are not indexed by search engines. However, the Deep Web encompasses more than just sites that cannot be accessed directly via traditional search engines. It also includes Internet content that meets any of the following criteria:

1. Inaccessible to current conventional search engines.
2. Accessible only for targeted queries or keywords.
3. Protected from search engine crawlers.
4. Protected by security mechanisms (login ID, password).
5. Protected by a logical or encrypted structure that is inaccessible from outside.

After the year 2000, Internet search engines improved so that they could collect information from databases of dynamic internet pages. Bergman in his work estimates that the Deep Web is 500 times larger than the surface network. It is assumed that the surface network is only 0.25 to 5 percent of the total Internet. The estimate of the size of the Surface Web is based on the data obtained by monitoring the status of the Internet. Currently, the Internet is used by slightly more than 5.46 billion users, while in the same period of 2016, the number of Internet users was 3.48 billion (Country Cassette – Real Time World Statistics 2022), (Denic 2017). Internet users have grown by about 57% in the last 6 years, making it the fastest-growing multinational shared domain. This multinational domain is part of the world's information domain, economy, state apparatus, army, etc. To protect their national interests, governments are legalizing control of the Internet on their territory and beyond. This control has already been established by various actors.

The first example of a state that controls activities on the Internet is the Russian Federation. The Russian government established control over all electronic

communication in 1996 (Blake 2016). The System for Operative Investigative Activities – SORM [*Система технических средств для обеспечения функций Оперативно − Розыскных Мероприятий − СОРМ*] is a system that all service providers must implement. The SORM is a set of equipment that allows the Federal Security Service of the Russian Federation [*Федеральная служба безопасности Российской Федерации – ФСБ*] – (FSB) to duplicate traffic from communication equipment or to provide access to the email servers and copy data. This system monitors mobile and fixed telephone communications, monitor internet communications and collects data on all types of communications, and stores them for up to three years.

The second example is, certainly, the United States of America, which, at the same time as the Russian Federation, carries out similar activities. The National Security Agency NSA implemented the Planning Tool for Resource Integration, Synchronization, and Management – PRISM to collect data from the US service providers. Before that, the *Upstream* program was used for tapping international cables that were crossing US territory. More about these programs and the confidential presentations that Edward Snowden gave to journalists in 2013 can be found on *The Washington Post* website (The Washington Post 2013).

Given that the data of Internet users are in any case controlled by the state authorities of their country or by the security services of foreign countries, a significant number of Internet users began to look for new network services on the Internet that would provide them with a certain level of privacy and security.

The Deep Web was one of the solutions to get out of the controlled network environment of the Surface Web. At the beginning, users protected their privacy by using virtual private network services − VPN and Proxies. In the period before 2001, the Freedom Network from Zero − Knowledge System, Inc. was a privacy-protected service. It was a commercial service and was used only by those who could afford to pay for service. Since the use of the service was not free, this service did not experience expansion throughout the globe.

One of the contemporary projects, aimed to protect privacy and increase security on the Internet, is The Onion routing − Tor. The project started on September 20, 2002. Tor is a routing protocol that enables anonymity in end-to-end routing. Network watchdogs, network operators, or government officials are not able to determine the type of communication, the source, and the destination of data sent over the network. It should be noted here that it is possible to see that a user is using Tor, but his activities cannot be seen, nor can the activities and identity of the user accessing the services be revealed on the server of the hidden services. This network is supported by volunteers who maintain the 'relays' and 'bridges' in the network and they donate their data flow and processing power to the needs of the network's functioning. The network was primarily developed for the US Navy, but after the program was abandoned and transferred to the hands of volunteers, there was a mass use and improvement of the service. According to data from the website *torproject.org*, the users of this network are:

1. People who seek to protect their privacy.
2. Journalists and their audience.

3. Law enforcement officers.
4. Activists and whistleblowers.
5. High and low-profile people.
6. Business executives.
7. Bloggers.
8. The military.
9. IT professionals.

The official Tor website does not list all users of this service. The advantages provided by hidden services, primarily end-to-end anonymity, and cheap and high-quality data encryption, are extremely attractive to people who do not care much about legality, ethics, and the prosperity of mankind. Due to surveillance on the surface network, they begin to use hidden services to spread a variety of illegal activities and take advantage of the opportunities that the network provides. In the part of the Deep Web, hidden website links provide access to adult content, material distributed by pedophiles, immoral forums, chat services, terrorist training, and recruitment material, fundraising for illegal activities, human and organ trafficking, and the black market (drugs, weapons, hiring assassins, etc.). This illegal part of the Deep Web is called the Dark Web. The Dark Web can be defined as a part of the Deep Web that contains generally illegal and anti-social information that can be accessed either through conventional or specialized internet browsers or software using a secret internet link (Dilipraj 2014).

3. The impact of the Dark Web in the fight against terrorists

The Dark Web was seen as an ideal ecosystem for Islamic State in Iraq and the Levant-ISIL (Berton 2015). In November 2015, after the attacks in Paris, ISIL used the hidden services of the Dark Web to spread propaganda. There are three main reasons for this.

First, they want to avoid censorship of their web pages on the Surface Web.

Second, the content of web pages on the Dark Web can only be accessed if data is available on the method of access, and the network itself protects the identity of persons who wish to access information on the pages or administer those pages or services.

Third, the content on the Dark Web is protected from hacker activities. The terrorist attack on Paris in 2015 triggered the Anonymous group to launch the hacker attack 'Operation Paris' (Blake 2015). The result of the operation was the removal of hundreds of websites on the Surface Web that were linked to ISIL. Unfortunately, websites have not completely disappeared from the Internet, because administrators have migrated them to the Dark Web. To continue accessing the pages, a link was published through the Telegram application that was a link to the dark web, using Tor technology, to the pages '*.onion'*.

One of the important activities that terrorist organizations use the Dark Web for is fundraising and the anonymous transfer of funds for the market of weapons, opiates,

hiring hitmen, and other trade in illegal goods and services. Fundraising using the Dark Web combined with anonymous transactions provided by cryptocurrencies increases the actors' resistance to the detection and seizure of funds. Cryptocurrencies, such as Bitcoin-BTC, and lately the increasing primacy in anonymous transactions Monero-XMR, have a significant role in massing users who want anonymity on the Internet (Rudes 2020). XMR is currently considered the cryptocurrency that provides the highest degree of privacy and anonymity. The transactions of this cryptocurrency are almost impossible to track, and this is one of the reasons why XMR is the choice of persons or actors who are engaged in illegal trade or concealment of income to avoid taxes.

Cryptocurrencies behave in payments in the same way as cash. It is very difficult to track such transactions because there is no official intermediary, a bank that mediates transactions. When there is an official intermediary in the transaction, he as a party to the business must submit data on the transactions based on a court order to the investigating authorities.

For example, the website "Fund the Islamic Struggle without Leaving a Trace" existed on the Dark Web for all donors who were willing to anonymously fund the holy war *Jihad* in BTC currency (Weimann 2016).

The black market on the Dark Web is full of web stores for the trade of drugs, weapons, ammunition, lethal means, forged IDs, personal data, duplicate payment card data, banned books, etc.

The next example of how terrorist organizations use the Dark Web is the case of a small terrorist cell from Indonesia. In addition to organizing fundraisers on the Dark Web, terrorists used stolen Personally Identifiable Information-PII, also provided through the Dark Web, for stock trading on the Forex webpage. This group managed to collect about US $600,000 with well combined several cyber criminal activities (Weimann 2016).

One of the most famous sites for trading illegal goods is The Silk Road 2.0. The arrest of the site's administrator only temporarily closed the trade in illegal items on the Dark Web, but sellers and buyers quickly found alternatives. Silk Road 2.0, an illegal internet trading site on the Dark Web, is an example of profitably taking advantage of the Dark Web to make money. Similar to e-commerce sites on the Surface Web, the Silk Road 2.0 site offered a wide range of illegal items (opiates, weapons, contract killing services). This website was the guarantor of the transaction between the buyer and the seller. A customer who would order illegal items from the Silk Road 2.0 site would pay for the items in the cryptocurrency BTC. The money would remain in the site's possession until the customer receives the goods. When the buyer receives the goods Silk Road 2.0 transfers funds to the seller in cryptocurrency. Certainly, for these transactions, the Dark Web site took a commission of 8 to 15 percent. The FBI estimated that the site had about 150,000 anonymous users and about 4,000 sellers. The value of the total trade until July 2013, when the website was discovered, was over US $1.2 billion (Sui, Caverlee, and Rudesill 2015). It may be assumed that part of the profits from the sale of illegal goods ended up in the hands of terrorists around the world.

The kill list is a very interesting example of the psychological effects on persons working in government institutions. Namely, the kill list was published between March and May 2016 by three pro-Islam hacker groups (SITE Intelligence group 2016). The kill list contained information on US citizens and government officials who are marked for execution. This operation was to wake up the 'lone wolves' who should carry out the execution. For the execution of persons from the kill list, the 'lone wolves' would receive a monetary reward in cryptocurrencies, which was specifically defined for each person individually. The link to access the data has been extended through the Telegram service. The personal data of individuals on the kill list were not obtained by these hacker groups but were bought on the Dark Web market from hackers who made a material profit by stealing and selling PII from social networks without knowing what the data would be used for later (Pearson 2016).

4. The impact of the Dark Web on the global information environment during the Covid-19 pandemic

Internet pages, social networks, and forums play a significant role in shaping perception, opinion, and behavior in crises. In the period of the global crisis caused by the Covid-19 virus infection, disinformation, although it seemed to be harmless by nature, could and did pose a great threat to global security. Internet sites where conspiracy theorists shared semi-truths and lied about security measures, and the origin of viruses and vaccinations quickly fell under state censorship around the world. As with Operation Paris, in this case, citizens who are supporters of conspiracy theories continued their search for information and the spread of disinformation on the pages of the Dark Web. Due to censorship on the Surface Web, there was a migration of pages from the surface to pages of the Dark Web. The information posted on the pages of the Dark Web becomes extremely dangerous because most users accept it as authentic and more accurate than the information provided by government authorities (Topor and Shuker 2020). When you add to this the anonymity in the interaction that the network provides to users, their trust in shared information increases even more, and the Dark Web becomes an environment for creating a global polarization of society into those who trust state authorities and those who do not and are already organized as internet clans. Although it is believed to be a small percentage of the population globally used the Dark Web for discussions and exchange of 'information', there are always physical circles of these people who could spread this disinformation very easily.

To determine the percentage of the population that used the Dark Web, there is a study on The use of the Dark Web as a Covid-19 information source: A three-country study was conducted (Sirola, Nuckols, Nyrhinen, and Wilska 2022). The results of the study show that a certain percentage of citizens of three countries (Finland, Sweden, and the United Kingdom) used the Dark Web as a source of information during the Covid-19 pandemic. In the United Kingdom, 19 % of the total sample searched for information on the Dark Web. Persons who have used the Dark Web

fit the following profile: young people who have advanced knowledge in the use of internet technologies.

In the middle of the period of the Covid-19 pandemic, websites for the trade of prohibited substances were also unavoidable. One example is the vaccine trade long before the vaccines were approved. One of the pages for e-commerce on the Dark Web had an advertisement for the sale of vaccines in cryptocurrencies at a price equivalent to US $5,000. That advertisement not only spread misinformation but also put the health of people who buy such untested substances at risk (Topor and Shuker 2020). Websites were selling illegal items and offered protective masks, and drugs such as chloroquine, hydroxychloroquine, and azithromycin. The offer included instructions for business subjects of Western countries to collect money from the state due to the Covid-19 pandemic, Internet domains that have connections with a corona in their names, medical devices that allegedly detect Covid-19, tests to confirm Covid-19, infected blood, false medical records about the virus and ventilators.

5. The impact of the Dark Web during the conflict in Ukraine and the global threat

Illegal e-commerce services are used on the Dark Web and in the latest conflict between Russia and Ukraine. An advertisement appeared on one of these services about the sale of the American-made anti-tank missile Javelin. On the trading webpage, this rocket was being sold at a price of US $30,000 (the actual regular price of a rocket like this is around US $200,000). Payment for this weapon has to be done in cryptocurrency around XMR150.05 (AtlasNews 2022). The seller, who is allegedly from Kyiv, claimed that he could provide the transport of the ordered goods to Poland, an EU country. It is still too early to determine if this is a real offer of anti-tank weapons or if it is part of Russian propaganda. What is certain is that such activities, even though they are on the Dark Web, have an impact on the global information environment. The Russian side uses this offer for an information campaign to influence public opinion in Western countries. The main message that the Russian side sends to the Western public is that although they donate weapons and equipment, it ends up on the black market and that taxpayers' money ends up in the pockets of war profiteers. On December 9, 2022, Russia requested an urgent session of the UN Security Council, at which the Russian ambassador to the UN stated that the weapons supplied by Western countries to Ukraine are increasingly ending up in the hands of terrorists not only in Europe but also in Africa and the Middle East. On the other hand, Ukraine treats the appearance of the sale of donated weapons on the Dark Web as part of Russian propaganda aimed at undermining the trust of Western public opinion in the Ukrainian government (FOXBusiness 2022).

The activities of hackers are fully in line with the actions of the countries they operate from. Before the conflict in Ukraine, Russian hackers had a code of not attacking countries that emerged from the USSR. After the conflict, from February 24, 2022, geopolitical tensions were also reflected in the Dark Web and hackers from

both sides started online activities outside the code. Groups of hackers often use forums, websites where information is posted (paste sites), applications for secure communication (Telegram, Signal...), and finally, specially built websites that support the actions they carry out and serve to plan the activities of each party. The available means of communication often serve hacker groups in the current conflict to communicate sensitive information to the other party and to agree and plan future online activities. When we talk about the disclosure of sensitive information, information related to government agencies, the army, political bodies, but also private companies, and groups that are connected to the parties to the conflict, are published in a targeted manner. On the black market of the Dark Web, the Russian hacking group Free Civilian offers for sale data from the databases of state institutions of Ukraine that have been the object of hacking attacks. Among these data are data from the electronic administration service https://diia.gov.ua/ [*Державні послуги онлайн*], the Ministry of Internal Affairs https://wanted.mvs.gov.ua/ [*Міністерство внутрішніх справ України*] and the like (Webz.io 2022)

In addition to PII, links to confidential documents belonging to the operational command 'North' of the Army of Ukraine were posted on one of the more popular Russian hacker forums, *xss.is*. On the opposite side, a cyber attack on Russian Federation security services information systems exposed vast amounts of data (Gioe 2022). The Shadow Hunters hacker group, from Ukraine, used the service *https://pastebin.com* to post information (paste sites) and anonymously distributed a large number of internet addresses that need to be attacked during the hacking operation. Among the pages defined as targets has been the page of the Russian president *http://20.kremlin.ru* and pages linked to the *kremlin.ru* domain.

The market of the Dark Web is an ideal place for hackers who possess knowledge that they can easily monetize. When they do that, they do not think about the consequences, but only about the profit made by selling sensitive data. Disclosure and sale of data on the critical infrastructure of companies, especially data on nuclear facilities and data on people who possess information on essential production processes brings profit to the persons who sell but increases the degree of endargenment of persons and objects. Cyble, a company that monitors the Dark Web, notes that the number of cyber attacks on nuclear facilities around the world is increasing. Western analysts cite the reason for the increase in attacks as a consequence of Russia's intervention in Ukraine. Beginning in February 2022, about eight disclosures of critical information appeared on cyber forums on the Dark Web. The leaked data related to nuclear facilities in Russia, Brazil, Iran, Taiwan, Indonesia, Thailand, India, and South Africa (Lapienytė 2022). Although nuclear facilities have air-gapped networks, the assumption is that the attacks were successful because they took advantage of network misconfigurations, exposed network elements, vulnerabilities in network control systems, and social engineering. The data that appeared on the Dark Web were internal nuclear plant documents, source codes of software used by energy companies, information on key nuclear plant personnel, construction plans, and details of plant equipment. This data is a so-called gold mine for future attackers. They are key to developing specialized malware, auditing controller firmware, and gaining access to organizations dealing with nuclear facilities.

6. Conclusion

The Dark Web allows users the service of complete anonymity and ensures a high degree of encryption of the information exchange. The diversity and possibility of combining different services and electronic tools increase the operational security of users and reduce the possibility of government authorities identifying actors. The Dark Web services are a reflection of the real situation on the physical global stage and are used by non-state and state actors. The variety of possibilities that the Dark Web provides to users does not mean that it is a 'silver bullet' against state institutions, law, and order. Some examples show that it is possible to identify service users and geolocate servers that provide services. Exposing service users and administrators is always due to non-compliance with operational security measures. However, serious actors when working on the Dark Web apply the measures. Tools to access the Dark Web do not have technical flaws that can be exploited to expose actors and track their intentions.

The Dark Web was and is a platform for psychological and information operations, propaganda dissemination, online indoctrination, recruitment and mobilization, virtual training, planning, and coordination of cyber operations, arms trading, trading of essential information on critical infrastructure and information on people who possess knowledge of certain technologies, to collect funds, financial fraud with personal data.

The migration of a growing number of users from the Surface Web to the Deep and Dark Web and the development of services that increasingly provide full protection of actors creates an environment in which the sources of the threat are uncertain, the motives of the actors are hidden or masked, and new threats do not have the same patterns as the previous ones. In such an environment, it is difficult to get the right information, make assumptions, perform analyses, and define tactics, techniques, and procedures as responses to threats.

Threats coming from the Dark Web have a global impact on the information environment and their diversity is the product of the adaptation of the Dark Web to the needs of the physical environment and geopolitical circumstances.

Addresses:
Nenad V. Denic
Miljana Miljanica 7/20
Belgrade, Serbia
War College
School of National Defense
University of Defense
Veljka Lukica Kurjaka 33
Belgrade, Serbia
E-mail: nenad.denic@vs.rs
Tel.: +381641985155

Sasa Devetak
Djure Danicica 2/17
Pancevo, Serbia
Department of Social Sciences and Humanities
Military Academy
University of Defense
Veljka Lukica Kurjaka 33
Belgrade, Serbia
E-mail: sasa.devetak@va.mod.gov.rs
Tel.: +381600770200

References

60 Minutes CBS News (2015) "New search engine exposes the 'dark web'". *CBS News,* 8 February. Available online at <https://www.cbsnews.com/news/new-search-engine-exposes-the-dark-web/>. Accessed on 05.12.2022.

AtlasNews (2022) "American FGM-148 Javelin appears on Dark Web marketplace". 2 June. Available online at <https://theatlasnews.co/conflict/2022/06/02/american-fgm-148-javelin-appears-on-dark-web-marketplace/>. Accessed on 08.12.2022.

Bergman, M. K. (2001) "The Deep Web: surfacing hidden value". *Journal of Electronic Publishing* 7, 1. DOI: https://doi.org/10.3998/3336451.0007.104

Berton, B. (2015) *The dark side of the web: ISIL's one-stop shop?* The European Union Institute for Security Studies (EUISS). Available online at <https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_30_The_Dark_Web.pdf>. Accessed on 07.12.2022.

Blake, A. (2015) "#OpISIS and #OpParis: Anonymous hacktivists to retaliate against ISIS after Paris attacks". The Washington Times, 16 November. Available online at <http://www.washingtontimes.com/news/2015/nov/16/opisis-and-opparis-anonymous-hacktivists-to-retali/>. Accessed on 07.12.2022.

Blake, A. (2016) "Russia weighs letting telecoms use govt. surveillance system for new anti-terror law: reports". The Washington Times, 10 August. Available online at <http://www.washingtontimes.com/news/2016/aug/10/russia-weighs-letting-telecoms-use-ex-kgbs-surveil/>. Accessed on 06.12.2022.

Bracci, A., M. Nadini, M. Aliapoulios, D. McCoy, I. Gray, A. Teytelboym, A. Gallo, and A. Baronchelli (2021) "Dark Web marketplaces and COVID-19: before the vaccine". *EPJ Data Science* 10, 6. DOI: https://doi.org/10.1140/epjds/s13688-021-00259-w

Denic, N. V. (2017) *Government activities to detect, deter and disrupt threats enumerating from the Dark Web*. M.M.A.S Thesis. Fort Leavenworth, Kansas.

Department of the Army, Army Regulation 530–1 (2014) *Operations Security*. Washington DC: Government Printing Office.

Dilipraj, E. (2014) "Terror in the Deep and Dark Web". *Air Power Journal* 9, 3, 121–140.

FOXBusiness (2022) "US officials push back on reports of dark web javelin missiles: 'Russian disinformation'". 4 June. Available online at <https://www.foxbusiness.com/politics/darkweb-javelin-missiles-russian-disinformation>. Accessed on 08.12.2022.

Gioe, D. V. and W. Styles (2022) "Vladimir Putin's Russian world turned upside down". *Armed Forces & Society*. DOI: https://doi.org/10.1177/0095327X221121778

Jarmon, J. A. (2020) *The new era in U.S. national security: challenges of the information age.* Lanham, MD: Rowman & Littlefield.

Lapienytė, J. (2022) "Nuclear sector threatened by data leaks on the dark web". Cybernews, 21 November. Available online at <https://cybernews.com/cyber-war/nuclear-data-leaks/>. Accessed on 08.12.2022.

Pearson, J. (2016) "These so-called 'ISIS kill lists' are a great reminder to change your password". Vice, June 16. Available online at <https://www.vice.com/en/article/qkj3j3/these-so-called-isis-kill-lists-are-a-great-reminder-to-change-your-password>. Accessed on 11.12.2022.

Rudes, J. (2020) "Monero becomes standard currency of the black market and breaks record". BitCoin Dynamic, 6 September. Available online at <https://bitcoindynamic.com/news/monero-becomes-standard-currency-of-the-black-market-and-breaks-record/>. Accessed on 07.12.2022.

Sirola, A., J. Nuckols, J. Nyrhinen, and T.-A. Wilska (2022) "The use of the Dark Web as a Covid-19 information source: a three-country study". *Technol Soc*, August, 70:102012. DOI: https://doi.org/10.1016/j.techsoc.2022.102012

SITE Intelligence group (2016) *SITE Intelligence group, Dark Web & Cyber security*. Available online at <https://sitemultimedia.org/docs/SITE_Analysis_of_Islamic_State_Kill_Lists.pdf>. Accessed on 11.12.2022.

Statcounter Global Stats (2022) *Search engine market share worldwide*. Available online at <https://gs.statcounter.com/search-engine-market-share>. Accessed on 05.12.2022.

Sui, D., J. Caverlee, and D. Rudesill (2015) *The Deep Web and the Darknet: a look inside the Internet's massive black box*. Wilson Center. Available online at <https://www.wilsoncenter.org/publication/the-deep-web-and-the-darknet>. Accessed on 07.12.2022.

The Washington Post (2013) "NSA slides explain the PRISM data-collection program". 6 June. Available online at <https://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/>. Accessed on 06.12.2023.

Topor, L. and P. Shuker (2020) "Coronavirus conspiracies and dis/misinformation on the Dark Web". *E-International Relations*, 9 October. Available online at <https://www.e-ir.info/2020/10/09/coronavirus-conspiracies-and-dis-misinformation-on-the-dark-web/>. Accessed on 06.12.2023.

UN Meetings Coverage and Press Releases (2022) "Effective arms-control measures needed to block diversion of Ukraine weapons, senior United Nations disarmament official tells Security Council". 9 December. Available online at <https://press.un.org/en/2022/sc15136.doc.htm>. Accessed on 10.12.2023.

Webz.io. (2022) "The Russia-Ukraine cyber war in the Deep and Dark Web". 9 March. Available online at <https://webz.io/dwp/the-russia-ukraine-cyber-war-in-the-deep-and-dark-web/>. Accessed on 08.12.2023.

Weimann, G. (2016) "Terrorist migration to the Dark Web". *Perspectives on Terrorism* 10, 3, 40–44. Stable web-address: https://www.jstor.org/stable/26297596