DARK WEB – BLACK DEEP BETWEEN PAST AND PRESENT

Hatidža Beriša, PhD[1]
University of Defence, Belgrade, Serbia

Katarina Jonev Ćiraković, PhD Candidate
Aleksandar Ćiraković, PhD Candidate
Faculty of Political Science, University of Belgrade, Serbia

BLACK DEEP WEB AS A CHALLENGE - DARK WEB

Dark Web[2] - black deep network, a space on the global network-Internet, is a logical structure that protects the identity of network users and hides the user's activities on the network. In the era of 5D warfare (disinformation, deception, destabilization, disruption and tailored destruction) the impossibility of personal identity and the possibility of a negative impact on the security of the state are ubiquitous. In the era of counter-terrorism, the dark web was the ICT infrastructure that provided security to terrorist organizations and activists. Such a network provided users with complete anonymity and very good and cheap crypto-protection. Combined with cryptocurrencies, the dark web was a space for terrorist indoctrination, recruitment, propaganda and training. "In the period of the fight against CoVid–19, the dark web services had a significant impact on the information environment and were a place for the spread of propaganda, conspiracy theories and the sale of media stones for the treatment of CoVid–19. During the conflict between Russia and Ukraine, the deep black network and the services it provides have an impact on shaping the information environment of the conflicting parties, but it can be said that it has an impact on the global information environment. The black deep network as a network for protecting the identity and activities of actors in the cyber domain represents a global security challenge in the fight against terrorism, during the CoVid–19 pandemic and in modern conflicts" (Denic, Devetak, 2023).

THE QUEST FOR SECURITY AND ANONYMITY ONLINE

The Internet as a network of all networks should provide all users with the same rights and opportunities. However, the Internet should also provide a certain level of security and anonymity to its users. The level of anonymity and security has been declining since 2000. States are increasingly exercising control in cyberspace to increase security in the physical domain.

The average internet user finds services on the Internet thanks to the internet search engines. The internet search engines such as Google, Bing, Yahoo, Baidu, Yandex, Ask are of great help to the internet users because data are searched through them. The popularity of the search engine 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 browser, while devices with the Micro-

1 berisa.hatidza@gmail.com

2 What is the dark web? The dark web is 6% of the deep web layer. The dark web is not the secure layer. Instead, it is a hidden layer of the deep web and is mostly used for illegal activities like cybercrimes, theft, smuggling, and terrorism.

soft operating system use the default Bing. The most popular internet search engines in the world for all platforms (mobile phone, tablet, desktop, laptop) based on the Statcounter GlobalStats website is Google with 92.20% share, while the second is Bing with 3.42% share (Statcounter Global Stats 2022).

Internet browsers use automated processes to collect as much data as possible on the Internet. Specialized programs analyze databases that are created on the basis of indexed words for each document for which data have been collected. When the user searches for a specific term, the pre-stimulators use their own algorithms to check the database and return information about the term to the user. 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 in order to make the page visible to as many users as possible. In most cases, website administrators optimize their pages so that search engines rank them higher when the algorithm sends information to the user. The average internet user thinks that the Internet is only what he can find using some of the internet search engines. However, the Internet is much larger than websites can index. The total percentage of indexed data on the Internet is estimated at about 5% (60 Minutes CBS News 2015). "The rest of the unindexed web pages are called the deep web, hidden web, or invisible web. The mentioned estimate of 5% is based on the total Internet traffic" (Denic, Devetak, 2023).

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 that cannot be indexed by conventional web browsers appear. A static website is linked to a single location on the Internet and the data on that page change from time to time. On the other hand, dynamic internet pages are more complex and the only thing that is sometimes constant is the page frame, while the data on the page depend on the data that the user requests. These pages are created based on the data requested by the user and are populated from related sources requested by the user. Dynamic pages are becoming more and more common, and therefore the unindexed part of the space between what is visible and what is invisible on the Internet begins to grow. In 1994, the term invisible web was introduced. The term refers to the information that was not visible to conventional internet browsers for that time period (Bergman, 2001).

The term invisible network had been used until 2001, when Michael K. Bergman introduced the new term - deep web in his work "The deep web: Surfacing Hidden Value". The antonym of the deep web becomes the surface web, which was previously called the visible web. The surface network is the part that the average internet user considers to be the Internet.

The deep web does not only represent internet pages that cannot be accessed directly through conventional browsers. The deep web represents content on the Internet that is:

1) Inaccessible via conventional internet browsers,
2) Accessible only through targeted queries or keywords,
3) Protected from algorithms used by internet browsers,
4) Protected by security mechanisms (user accounts, passwords...),
5) Protected by a logical or encrypted structure that is inaccessible from the outside (Denić, Devetak,2023).

After the year 2000, internet browsers improved so that they can collect information from databases of dynamic internet pages. In his work Bergman (Bergman) estimates that the deep network 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 Internet 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). The number of internet users has grown by about 57% in the last 6 years, which makes it the fastest growing multinational shared domain. This multinational domain is part of the world information domain, economy, state apparatus, army, etc. In order to protect their own national interests, countries are trying to legalize the 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, which has controlled all electronic communications on its territory since 1996 (Blake, 2016). The system of operational investigative activities [Sistema tehnicheskih sredstv dlya obespecheniya funktions Operativno-Rozysknykh Meropriyatij-SORM] is a system that all providers of telecommunication services must have. SORM is equipment that allows the Federal Security Service of the Russian Federation-FSB to duplicate user traffic and store it for its own needs. This system monitors mobile and landline telephone communications, monitors internet communications and collects all data of all types of communications as target data and stores them for up to three years.

Another example is of course the United States of America, which carried out similar activities at the same time as the Russian Federation. The National Security Agency (NSA) has implemented the Planning Tool for Resource Integration, Synchronization, and Management (PRISM) to collect data from telecommunications service providers in the US. Prior to that, the Upstream program had been used to eavesdrop on international lines passing through US territory. More about these programs and the highly offensive presentations that Edward Snowden gave to journalists in 2013 to show what the US was doing can be found on the website of The Washington Post (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 totally controlled network environment of the surface internet. In the beginning, users protected their privacy by using virtual private network services [Virtual Private Network–VPN] and proxy programs. In the period before 2001, The Freedom Network from Zero–Knowledge System, Inc. was a privacy network. It was a commercial service and was used only by those who could afford to pay for such a service. Since the use of the service was not free, this service did not experience expansion throughout the globe.

Another project, which 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 cannot determine the source and 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 needs of 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 want to protect their privacy,
2) Journalists and their readers,

3) Security authorities,
4) Activists and whistleblowers,
5) Persons of high and low "profile",
6) Directors of companies,
7) Bloggers,
8) Army,
9) IT experts (Denić, Devetak,2023).

The official Tor website does not list all users of this anonymity service. The advantages provided by hidden services, primarily end-to-end anonymity, 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 the 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 Internet via hidden Internet links, adult content, material distributed by pedophiles, immoral forums, chat services, training and recruitment material for terrorists, fundraising for illegal activities, human and organ trafficking, and the black market can be accessed (drinking, sneering, hiring assassins, etc.). This illegal part of the deep internet is called the dark web. The black deep 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 using a secret internet link (Dilipraj 2014:124).

THE POTENTIAL OF THE DARK WEB IN THE FIGHT AGAINST TERRORISTS

The dark web was considered an ideal ecosystem for Islamic State in Iraq and the Levant-ISIL's activities (Berton 2015). In November 2015, after the attacks on Paris, ISIL used the hidden services of the dark web to spread propaganda. There are three main reasons for this (Denić, Devetak,2023).

First, they want to avoid censorship of their internet pages on the surface network.

Secondly, the content of internet pages on the dark web can only be accessed if the data on the access method are available, and the network itself protects the identity of the persons who want to access the information on the pages in question or administer those pages during access to that content.

Third, the content on the dark web is protected from hacker activities. The terrorist attack on Paris in 2015 triggered the Anonymous hacktivist group to launch "Operation Paris" (Blake, #OpISIS and #OpParis: Anonymous hacktivists to retaliate against ISIS after Paris attacks 2015). The result of this operation was the removal of hundreds of websites on the surface network that were linked to ISIL. Unfortunately, websites did not completely disappear from the global Internet, but administrators migrated them to the dark web. In order to continue accessing the pages in question, the Telegram application published a link that was a link to the black deep web, using Tor technology, to the pages "onion".

One of the most important activities for which terrorist organizations use the black deep network is the collection of funds and the anonymous transfer of funds for the black market of weapons, opiates, ordering murder and other trade in illegal goods and services (Denic, 2017). Fundraising using the dark web combined with anonymous transactions provided by cryptocurrencies increases actors' resistance to detection and seizure of funds. Cryptocurrencies, such as for example 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 in order to avoid taxes (Denic, 2017).

Cryptocurrencies act the same as cash in the payment system. 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, that person as a party to the business, has the obligation to submit data on the transactions based on a court order to the authorities conducting the investigation.

For example, the website "Fund Islamic Struggle Without Leaving Traces" 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 black deep web is full of electronic stores for the trade of drugs, weapons, ammunition, lethal means, forged IDs, personal data, payment card duplicating 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 identity information, also provided through the dark web, for stock trading on the Forex surface network website (Pearson, 2016). This group managed to collect about 600,000 US dollars with several cybercriminal activities (Weimann, 2016).

One of the most famous sites for trading in illegal goods is The Silk Road 2.0. The arrest of the administrator of the site closed the trade in illegal items on the dark web only temporarily, but sellers and buyers quickly found alternatives. Silk Road 2.0, an illegal online trading site on the dark web, is an example of profitably taking advantage of the black deep web to make money. Similar to internet trading sites on the surface network, 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 remained in the possession of the site until the customer received the goods. When the buyer received the goods, Silk Road 2.0 transferred funds to the seller in cryptocurrency. Of course, the black deep web site took a commission of 8 to 15 percent for those transactions. The FBI estimated that the site had about 150,000 anonymous users and about 4,000 sellers. The value of total trade by July 2013, when the website was discovered, was over 1.2 billion US dollars (Sui, Caverlee and Rudesill 2015). It can 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 psychological effects on persons working in state 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 were to be killed. The aim of this operation was to wake up the "lone wolves" who should carry out the execution. For the execution of persons from the "lone wolves" kill list, they would receive a monetary reward in crypto-currencies, which was specifically defined for each person individually. The link to access the data was extended through the Telegram service. The personal data in the kill list were not obtained by those hacker groups, but were purchased on the black market of the deep web from hackers who made a material profit by stealing and selling personal data from social networks without knowing what the data would be used for later.

THE IMPACT OF THE DARK WEB ON THE GLOBAL INFORMATION ENVIRONMENT DURING COVID-19

Internet pages, social networks and forums play a significant role in shaping perception, opinion and behavior in crisis situations. In the period of the crisis caused by the CoVid−19 virus infection, disinformation could and did pose a great danger to security although it seemed to be harmless in nature. Internet sites where conspiracy theorists shared half-truths and lies about security measures, the origin of viruses and vaccinations quickly fell under state censorship around the world. As with the Paris operation, 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 black deep web. Due to censorship on the surface network, there was a migration of pages from the surface to pages of the black deep network. The information posted on the pages of the black deep web became extremely dangerous because most users accepted it as authentic and more accurate than the information provided by government authorities (Topor, 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 black deep network 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 that used the dark web for discussions and exchange of "information" globally, there are always physical circles of these people who could spread this disinformation very easily (Bracci, 2022). In order to determine the percentage of the population that used the black deep web, a survey on the use of the black deep web as a source of information for CoVid−19 was conducted by three countries (United Kingdom, Sweden and Finland) (Sirola, et al. 2022). The results of the study show that a certain percentage of citizens of these three countries used the black deep web as a source of information during the CoVid−19 pandemic. In the United Kingdom, 19 percent of the total sample searched for information on the dark web. Persons who used the dark web fit the following profile: young people who had advanced knowledge in the use of internet technologies.

In the age of the CoVid−19 pandemic, websites for the trade of prohibited substances were also unavoidable. An illustrating example is the vaccine trade long before the vaccines were approved. On one of the pages of the black deep web, there was an ad for the sale of vaccines in cryptocurrencies at a price equivalent to 5,000 US dollars. Such ads not only spread misinformation, but also put the health of people who bought such untested substances at risk (Topor, Shuker 2020). Sites selling illegal items offered protective masks, drugs such as chlorquine, hydrochlorquine and azithromycin (Jarmon, 2020). "The offer included instructions for business entities of Western countries to collect money from the state due to the CoVid−19 pandemic, internet domains that had connections with corona in their names, medical devices that supposedly detect CoVid−19, tests to confirm CoVid−19, fake medical documentation about the virus and respirators" (Denić, Devetak,2023).

DARK NETWORKS OPERATING DURING THE CONFLICT IN UKRAINE AND THE GLOBAL THREAT

Illegal sales services are used on the dark web in the latest conflict between Russia and Ukraine. An ad appeared on one of these services about the sale of American-made anti-tank missiles called Koplje [Javelin]. On the trading page, this rocket was being sold at a price of US$30,000 (the actual price of a rocket like this is around US$200,000). Payment for this weaponry was to be made in cryptocurrency

around 150.05 XMR (AtlasNews 2022). A seller from Kiev claimed that he could provide the transport of the ordered goods to Poland, an EU country. It is still too early to determine whether this is a real offer of anti-tank weapons or 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 is using this offer for the purposes of an information campaign in order to influence public opinion in Western countries. The main message that the Russian side sends to Western public opinion 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 were 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 state apparatus (FOXBusiness 2022).

The activities of hackers are fully in line with the actions of the countries from which they operate. Before the conflict in Ukraine, Russian hackers had a code of not attacking countries that emerged from the USSR. After the conflict started on February 24, 2022, geopolitical tensions were also reflected in the dark web and hackers from both sides started online activities beyond 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 state agencies, the army, political bodies, as well as private companies and groups that are connected to the parties to the conflict are published in a targeted manner. The Russian hacking group Free Civilian uses the black market of the deep web to offer 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/ [Deržavní poslugi online], the Ministry of Internal Affairs https://wanted.mvs.gov.ua/ [Mínisterstvo vnutríšních sprav Ukraí" ni] and the like (Webz.io 2022).

In addition to citizens' data, links to confidential documents belonging to the operational command "North" of the Army of Ukraine were posted on one of the most popular Russian hacker forums, xss.is.

On the other hand, the Shadow Hunters hacker group from Ukraine uses the service https://pastebin.com to post information and anonymously distributes a large number of Internet addresses that need to be attacked during the hacking operation. Among the sites defined as targets are the site of the Russian president http://20.kremlin.ru and sites linked to the kremlin.ru domain.

The black market of the deep web is an ideal place for hackers who possess knowledge that can easily be monetized. When they do that, they do not think about the consequences, but only about the profit made by publishing sensitive data. The disclosure and sale of the data on the critical infrastructure of companies, especially the data on nuclear facilities and the data on people who possess information on essential production processes bring profit to the persons who sell but increases the degree of endangerment 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. Pro-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 disclosed 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 deep black web ranged from internal documents of nuclear plants, source codes of software used by energy companies, information on key nuclear plant personnel, construction plans and details of plant equipment. Those data were the so-called gold mine for future attackers. They were key to developing specialized malware, auditing controller firmware, and gaining access to organizations dealing with nuclear facilities (Denic, Devetak 2023).

Since the beginning of the conflict, the effects on the information environment from cyberspace have not been forgotten even by countries that are not involved in this conflict. In order to influence public opinion and the economic conditions of the Republic of Serbia, anonymous reports appeared about the placement of bombs in elementary schools, state institutions and on flights between Belgrade and Moscow (Denić, Devetak, 2023). In accordance with the procedures in the Republic of Serbia, this type of threats must be checked by specialized teams in order to protect the civilian population. There is an assessment that these threats were created with the aim of changing the official state policy of the Republic of Serbia and the position of the Republic of Serbia regarding the conflict. The impossibility of identifying the source of the threat, as well as the territory from which the threatening electronic messages were sent, was achieved thanks to the high level of awareness of the application of operational security measures - OPSEC of the actors who generated the threat. Operational security is defined as the process of protecting sensitive and/or critical information from hostile reconnaissance and collection in a way that traditional security programs cannot protect. The method of applying the operational security of the actor will be described below. The source of the threat uses an e-mail exchange service, in this case Proton Mail was used as the service for sending messages. This service provides end-to-end protection of messages, does not require identification from the user when opening an account. The mentioned service protects the user's internet address, so that the source of the threat at a given moment cannot be geolocated based on the address. The advantage of this service is also in the laws of Switzerland (the server is located in Cern), which is neutral militarily and politically, all in order to protect free speech. With this service, as with other e-mail services (Google, Microsoft, Yahoo...), the company has the right to access electronic data on the server, but while popular providers of these services companies can access the data, Proton Mail data cannot be accessed by the company because it is encrypted and only the sender and receiver have the decryption data. It is certain that the threat addressed to institutions and companies in the Republic of Serbia is a terrorist act, and it would be logical for Proton Mail to provide data on the source of the threat at the request of the investigative authorities of the Republic of Serbia, which would only be possible in this case (Denić, Devetak,2023). Unfortunately, the source of the threat implements its own operational security measures. One of the operational security measures is to open an account and access the service through the deep web at the service address https://protonirockerxow.onion/. For the authorities of the Republic of Serbia, this is an approach from the black deep network, given that the threat is aimed at undermining the security of a sovereign state. Services that are combined in order to achieve complete operational security in cyberspace are Tor, Telegram, Signal, Pasteit, Pastebin, I2P

CONCLUSION

Based on the above, it is concluded that the Black Deep Network remains anonymous, especially taking into account that there is a high degree of crypto-protection of the exchanged information, which are reflected in the diversity and the possibility of combining different services and electronic

tools that increase the operational security of network users and reduce the ability of state authorities to identify actors. Black deep web services are a reflection of the real situation on the 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. There are examples that 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 in the dark web apply these measures. Tools to access the dark web do not have technological flaws that can be exploited to expose actors and track their intentions.

The various services of the Black Deep Network are particularly prominent, as well as the platforms for psychological and information operations, propaganda dissemination, online indoctrination, recruitment and mobilization, virtual training of actors, planning and coordination of cyber operations, arms trade, trade of essential information about critical infrastructure and information about people who have knowledge of certain technologies, to collect funds and commit financial fraud with personal data.

It is especially important to point out how much the transition from the surface to the deep and black deep network for all users and especially for the development of services provides opportunities for the complete 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 before, In such an environment, it is increasingly difficult to get the right information, make assumptions, perform analyses, define tactics, techniques and procedures as responses to threats.

The threats that come from the black deep web are a potential danger to the information environment and their diversity represents the adaptation of the black deep web to the needs of the physical environment and geopolitical circumstances.

REFERENCES

AtlasNews. *American FGM-148 Javelin Appears On Dark Web Marketplace.* 02 June 2022. https://theatlasnews.co/conflict/2022/06/02/american-fgm-148-javelin-appears-on-dark-web-marketplace/ (last visit May 8th, 2024).

Bergman, Michael K. "The Deep Web: Surfacing Hidden Value". *Journal of Electronic Publishing.* August 2001. https://doi.org/10.3998/3336451.0007.104 (last visit May 5th, 2024)

Berton, Beatrice. "The dark side of the web: ISIL's one-stop shop?" *The European Union Institute for Security Studies (EUISS).* June 2015. https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_30_The_Dark_Web.pdf (last visit April 5th, 2024)

Blake, Andrew. *#OpISIS and #OpParis: Anonymous hacktivists to retaliate against ISIS after Paris attacks.* 16 November 2015. http://www.washingtontimes.com/news/2015/nov/16/opisis-and-opparis-anonymous-hacktivists-to-retali/ (last visit April 12th, 2024)

Russia weighs letting telecoms use govt. surveillance system for new anti-terror law: reports. 10 August 2016. http://www.washingtontimes.com/news/2016/aug/10/russia-weighs-letting-telecoms-use-ex-kgbs-surveil/ (last visit May 10th, 2024)

Bracci, Alberto, et al. "Dark Web Marketplaces and COVID-19: before the vaccine". *EPJ Data Science.* 21 January, 2021. https://epjdatascience.springeropen.com/articles/10.1140/epjds/s13688-021-00259-w (last visit May 5th, 2024)

Country Cassette – Real Time World Statistics. *Internet Live Stats.* 06 December, 2022. https://countrycassette.com/internet-live-stats-2022/ (last visit March 3rd , 2024)

Denic, Nenad V. *Government activities to Detect, Deter and Disrupt threats enumerating from the Dark Web.* Fort Leavenworth, Kansas: M.M.A.S Thesis, 2017.

Denic, N, Devetak, Dark web – as challenge of te contemprory information age, Trames, 2023

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

Dilipraj, E. "Terror in the Deep and Dark Web". *Air Power Journal 9, no. 3*, 2014: 121-140.

FOXBusiness. *US officials push back on reports of dark web javelin missiles: 'Russian disinformation'*. 04 June, 2022. https://www.foxbusiness.com/politics/darkweb-javelin-missiles-russian-disinformation (last visit June 5th, 2024)

Jarmon, Jack A. *The New Era in U.S. National Security: Challenges of the Information Age.* Lanham, MD: Rowman & Littlefield, 2020.

Lapienytė, Jurgita. *Nuclear sector threatened by data leaks on the dark web.* 21 November 2022. https://cybernews.com/cyber-war/nuclear-data-leaks/ (last visit June 10th, 2024)

Pearson, Jordan. *These So-Called 'ISIS Kill Lists' Are a Great Reminder to Change Your Password.* 16 June, 2016. https://www.vice.com/en/article/qkj3j3/these-so-called-isis-kill-lists-are-a-great-reminder-to-change-your-password (last visit April 16th, 2024)

Rudes, Jorge. *Monero becomes standard currency of the black market and breaks record.* 06 September, 2020. https://bitcoindynamic.com/news/monero-becomes-standard-currency-of-the-black-market-and-breaks-record/ (last visit May 15th, 2024)

Sirola, Anu, Julia Nuckols, Jussi Nyrhinen, and Terhi-Anna Wilska. "The use of the Dark Web as a COVID-19 information source: A three-country study". *ScienceDirect.* August 2022. https://doi.org/10.1016/j.techsoc.2022.101977 (last visit June 5th, 2024)

SITE Intelligence group. "SITE Intelligence group, Dark Web & Cyber security". *SITE Intelligence group.* 17 June, 2016. https://sitemultimedia.org/docs/SITE_Analysis_of_Islamic_State_Kill_Lists.pdf (last visit June 15th, 2024)

Statcounter Global Stats. *Search Engine Market Share Worldwide.* November 2022. https://gs.statcounter.com/search-engine-market-share (last visit June 7th, 2024)

Sui, Daniel, James Caverlee, and Dakota Rudesill. "The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box". *Wilson Center.* October 2015. https://www.wilsoncenter.org/publication/the-deep-web-and-the-darknet (last visit May 5th, 2024)

The Washington Post. *NSA slides explain the PRISM data-collection program.* 6 June, 2013. https://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ (last visit June 10th, 2024)

Topor, Lev, and Pnina Shuker. "Coronavirus Conspiracies and Dis/Misinformation on the Dark Web". *E-International Relations.* 09 October, 2020. https://www.e-ir.info/2020/10/09/coronavirus-conspiracies-and-dis-misinformation-on-the-dark-web/ (last visit April 30th, 2024)

Webz.io. *The Russia-Ukraine Cyber War in the Deep and Dark Web.* 09 March, 2022. https://webz.io/dwp/the-russia-ukraine-cyber-war-in-the-deep-and-dark-web/ (last visit May 25th, 2024)

Weimann, Gabriel. "Terrorist Migration to the Dark Web". *Perspectives on Terrorism.* Terrorism Research Initiative, June 2016. 40-4