Cyber Influence Campaigns in the Dark Web

Lev Topor and Pnina Shuker

In recent years there has been a significant rise in the scope and intensity of information wars between the great powers and other forces in the international arena, and influence campaigns have become a legitimate tool in the hands of politicians, propagandists, and global powers. In this context, the professional literature has focused most on campaigns on social networks while it has almost ignored similar campaigns in the Dark Web where the current research tends to focus on criminal activity. The Dark Web was developed by the American Navy for intelligence purposes and was then promoted by the West as a public tool to protect privacy and anonymity. Today it provides fertile ground for deliberate leaks by countries that do not wish to publish certain information in the traditional media. These leaks are perceived as authentic, leading the media and other intelligence organizations to swallow the bait and investigate, and in some cases they even change their operations accordingly. The purpose of this article is to present the way in which the Dark Web is used in influence campaigns, particularly through deliberately leaking information.

Keywords: Dark Web, influence campaigns, propaganda, information wars, disinformation

Dr. Lev Topor is a senior strategic advisor and researcher on racism and cyber. Pnina Shuker is a Neubauer Research Fellow at the Institute of National Security Studies.

Introduction

In January 2019, tens of thousands of documents and emails from senior Russian government officials, leaders of the Russian Orthodox Church, and Russian oligarchs were leaked to the Dark Web. The leak appears to have been the outcome of activity by activist hackers ("hacktivists") who declared that they were not motivated by ideology but rather by the desire to ensure freedom of information: "We have no goal except to ensure that information is accessible to those who need it more than anyone—the people."[1] This incident shows how the Dark Web is being used to bypass the restrictions that totalitarian regimes place on freedom of expression. In addition, however, in recent years, many players on the international scene have been making use of the Dark Web to share deliberate, sometimes false, leaks in order to exercise political influence, highlighting the built-in tension that exists on the internet between the protection of privacy and the needs of national security.

Traditionally, the Dark Web has provided a convenient space for criminal activity, as well as for leaking and trading information. Recently the scope and intensity of the information wars conducted on the Dark Web between various elements in the international arena have increased significantly, with each side deliberately using leaks and disinformation to manipulate public awareness of the other side. The purpose of a leak may be purely military, or it may be intended to apply social or even commercial influence. For example, countries that do not wish to publicize certain things on traditional media can leak the information on the Dark Web, giving it the appearance of authenticity. Some media outlets have set up their own platforms to provide encrypted access as a way of encouraging leaks. Examples are WikiLeaks and Secure Drop, which are discussed in more detail below. The Dark Web is also a marketplace for malware, spyware, worms, and countless other malicious programs and files, as well as media encryption and cyber tools (such as PGP and other easy to use encryption guides).

This article aims to show how actors on the international stage are using the Dark Web to distribute propaganda and disinformation about their rivals, and how these actions can be translated into wide-reaching campaigns of influence. The article has three parts: The first part is a theoretical review of the manipulation of data in general and of influence campaigns in particular,

1 Stephan Jajecznyk, "The Dark Side of the Kremlin: Hacked Russian Documents Explained," *Al Jazeera*, February 25, 2019.

with several examples of important recent campaigns. The second part deals with the Dark Web, its characteristics, and chief uses. The third part, which synthesizes the findings of the first two, shows how the Dark Web is used to implement influence campaigns and its scope.

What Are Influence Campaigns?

An influence campaign is the coordinated, combined, and synchronized application of diplomatic, informational, military, and economic abilities, together with other national capabilities, whether in times of peace, periods of crisis, hostile situations, or following hostilities. The campaign seeks to influence the behaviors and decisions of target populations in other countries and persuade them to adopt positions that serve the interests of the campaign's initiators.[2] Campaigns to influence cognition are a familiar type of operation intended to serve a range of political, security, economic, and social ends. At the national level, influence campaigns are designed to achieve their aims, inter alia, by interfering with personal and economic security, undermining the public's trust in—and support for—national institutions and weakening social cohesion. The methods they use include active tampering with systems and processes; attempts to trigger actions or deter actions; obtaining information and using it to create messages; disseminating these messages and maximizing their effect. The channels for distributing messages include traditional media as well as new media, namely the internet and the social networks. Opinion leaders often serve as "unwitting agents" who make the messages more trustworthy and increase their reach.[3]

In recent years, there has been a marked rise in attempts by foreign elements (both governmental and non-governmental) to intervene in the election campaigns of rival countries using digital tools. Sometimes this involves cyberattacks on the computer systems supporting the electoral process (databases, software, and communications systems) in order to disrupt their operation or to distort or steal data. At the same time, extensive efforts are made to change the direction of public discourse in the target country and thus affect voting. The third type of influence campaign is a synthesis

2 Eric V. Larson, Richard E. Darilek, Daniel Gibran, Brian Nichiporuk, Amy Richardson, Lowell H. Schwartz, and Cathryn Quantic Thurston, *Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities* (Santa Monica: RAND Corporation, 2009), p. 2.

3 Ron Shleifer, "Psychological Warfare in Operation Cast Lead," *Ma'arachot*, no. 432 (August 2010): 19–20 [In Hebrew].

of the first two and uses cyber tools to penetrate the public consciousness. The possibilities are wide, ranging from attempts to undermine public faith in the democratic process, to interfering in support for specific parties or candidates. There have even been efforts to dissuade people from voting altogether, based on identity or socio-economic status.[4]

The main players behind these attempts at intervention in elections are authoritarian regimes, such as Russia, China, and Iran. Even some democratic-liberal governments, such as the United States, Britain, and also Israel, use these methods of influencing events in the international arena. For example, Russia has a long tradition of exploiting influence campaigns and has developed a systematic doctrine and operational capabilities for this purpose.[5] In this context, Russian methods include spreading false news on social networks by means of fake profiles; acquiring genuine profiles as a vehicle for political messages in support of pro-Russian candidates in elections worldwide, or to publish false or even incriminating information about Moscow's enemies, using Kremlin-owned media to manipulate news reports.[6] In the last six months alone, Russia has conducted influence campaigns for manipulating elections, including in Spain, Nigeria, Indonesia, and South Africa, among others, as well as in the elections to the European Parliament.[7]

China also makes widespread use of propaganda and influence campaigns, both as a way of shaping the image of the Chinese communist party and in undermining the stability of its rivals.[8] Reports have increasingly looked at China's attempts to interfere with elections in other countries, such as Sri Lanka, Malaysia, and Australia.[9] In addition, just before the US mid-term elections, the Trump administration announced that China, Iran, and Russia

4 Chris Tenove, Joran Buffie, Spencer McKay, and David Moscrop, *Digital Threats to Democratic Elections: How Foreign Actors Use Digital Techniques to Undermine Democracy* (Vancouver: Center for the Study of Democratic Institutions, University of British Columbia, 2018), p. 2.

5 Dima Adamski. "The Art of Cybernet Operations: From the Viewpoint of Strategic Studies and a Comparative Perspective," *Eshtonot*, no. 11 (2015): 28–48 [in Hebrew].

6 Alina Polyakova, "Want to Know What's Next in Russian Election Interference? Pay Attention to Ukraine's Elections," Brookings, March 28, 2019; Michael Schwirtz and Sheera Frenkel, "In Ukraine, Russia Tests a New Facebook Tactic in Election Tampering," *New York Times*, March 29, 2019.

7 Pnina Shuker, "Foreign Intervention in Elections Worldwide: Traits, Trends, and Lessons for Israel," *INSS Insights*, no. 1173, June 10, 2019.

8 Erica Pandey, "How China Became a Global Power of Espionage," *AXIOS*, March 23, 2018.

9 Prashanth Parameswaran. "China's Influence Operations in Asia: Minding the Open Door Challenge," *The Diplomat*, May 14, 2019.

together were trying to undermine the democratic process with an on-line propaganda campaign—including the spread of disinformation on social media—with the aim of deepening the ideological rifts in the United States and stirring up internal arguments about issues on the local agenda.[10] As part of its hostility to the United States, China is also trying to further its influence in Singapore: it was recently claimed that the Chinese communist party was contacting Singaporeans of Chinese origin, principally through the Chinese application "Wechat," in an attempt to influence politics and society in Singapore.[11] The Chinese are also reported to be using on an unprecedented scale the Facebook, Twitter, and YouTube platforms—all three banned in China itself—in order to defuse the fierce protests in Hong Kong against Chinese interference in local affairs.[12]

Iran is another country that does not refrain from using these methods. In August 2018, Twitter and Facebook deleted hundreds of accounts suspected of links to an Iranian disinformation campaign.[13] The content posted by these accounts was designed to highlight topics and narratives that suited Iranian foreign policy and promote its anti-Saudi, anti-Israeli, and pro-Palestinian agenda, and also to stimulate support for certain elements of US policy that serve Iranian interests, such as the 2015 nuclear treaty between Iran and the powers.[14] At the end of October 2018, a network of Facebook pages was found, which originated in Iran and was designed to influence public opinion in the United States and Britain.[15] There have also been increasing reports about Iranian cyberattacks and influence campaigns against Israel. At the end of January 2019, at a Cyber Tech conference, Prime Minister Netanyahu declared that Iran was trying to influence the elections in Israel by means of fake network accounts and was carrying out cyberattacks against Israel

10 Abigail Grace, "China's Influence Operations Are Pinpointing America's Weaknesses," *Foreign Policy*, October 4, 2018.

11 Muhammad Faizal Bin Abdul Rahman, "Foreign Influence in Singapore: Old Threats in New Forms," *The Diplomat,* July 23, 2019.

12 Raymond Zhong, Steven Lee Myers, and Jin Wu, "How China Unleashed Twitter Trolls to Discredit Hong Kong's Protesters," *New York Times,* September 18, 2019.

13 Craig Timberg, Elizabeth Dwoskin, Tony Romm, and Ellen Nakashima, "Sprawling Iranian Influence Operation Globalizes Tech's War on Disinformation," *Washington Post*, August 21, 2018.

14 Adriane M. Tabatabai, "A Brief History of Iranian Fake News: How Disinformation Campaigns Shaped the Islamic Republic," *Foreign Affairs*, August 24, 2018.

15 "Facebook Is Fighting Fake News from Iran: 'We've Destroyed a Propaganda Network – A Million Users Were Exposed,'" *TheMarker,* October 27, 2010 [in Hebrew].

"on a daily basis."[16] Contrary to the known Russian efforts, which exhibit a relatively high level of sophistication, Iranian and Chinese attempts to influence events are poorly executed and fairly easy to track.

Elections all over the world in the last six months have taken place in the shadow of suspected influence campaigns. Indeed, in many cases the campaigns were identified, particularly the Russian ones. Analysis of these efforts shows that counter moves by media giants and governments themselves reduced the foreign attempts to use bots as a tool for influence on social networks. On the other hand, today it is possible to identify growing activity by human influencers. Moreover, efforts to influence via the established media are again playing a significant role as well as through instant messaging applications, such as WhatsApp and Telegram, which have a higher level of credibility. Information is transferred on these closed platforms among relatively limited groups of family and friends, giving the messages the appearance of reliability. Moreover, the end-to-end encryption technology used by these platforms denies even their administrators access to the messages sent, unless a user reports some content as problematic. These features make it extremely difficult to track and remove any false information.[17]

The Dark Web: Characteristics and Uses

The Dark Web has become one of the most talked about subjects in the cybersecurity community.[18] To understand the formation and development of the Dark Web and its unique features, a short review of the regular internet is necessary. The Surface Web was part of a communications project of the United States Department of Defense in the 1960s, known as the Advanced Research Project Agency Network (ARPANET). In 1983, the closed network under the Network Control Protocol (NCP) was changed to an open network, now referred to as the Transmission Control Protocol or the Internet Protocol—TCP/IP.[19] Opening up the network led to a massive expansion of activity—from just a few connections to many millions—and

16 Stav Namer, "Netanyahu: Iran Is Making Cyberattacks on Israel on a Daily Basis," *Ma'ariv,* January 29, 2019 [in Hebrew].
17 Shuker, "Foreign interference in Global Elections."
18 Mihnea Mirea, Victoria Wang, and Jeyong Jung, "The Not So Dark Side of The Darknet: A Qualitative Study," *Security Journal* 32, no. 2 (2019): 102–118.
19 George Hurlburt, "Shining Light on the Dark Web," *IEEE Computer* 50, no. 4 (2017): 100–105.

to a split into categories of the national network (Class A), the regional network (Class B), and the local network (Class C), laying the infrastructure for the public internet we know today. The internet now links huge numbers of computers and devices through nodes or access points.[20]

The ARPANET project was officially closed in 1989, leaving behind the public areas: database addresses (internet pages) and accessible network protocols, browsers for the general public, and an accessible language (for example, the HTML language). In order to make the internet accessible for all, the Internet Corporation for Assigned Names and Numbers (ICANN) organization was established, which supplied addresses and network numbers and attached names to IP addresses. The organization began to index nearly all the services and public information and invited technology companies to build publicly accessible databases, such as Google, Bing, AOL, Yandex.ru, and others.[21] The result was that large corporations and governments were able to shape search lists as they wished and thus control which information was accessible to the public, essentially giving birth to the Deep Web.[22]

The Deep Web refers to any kind of information that is not mapped by search engines and to which access is restricted but can be obtained through ordinary (infrastructure) browsers, such as dynamic internet pages, unlinked internet pages, internet pages that are not based on HTML, and other restricted databases. Many security elements also set up private networks (such as LANs) and deep networks, such as the army or police networks, to which the general public does not have any access. At the same time, the Deep Web also contains private information, such as financial databases, biometric databases, medical data, and so on. For example, when a user enters his own bank account, he is entering the Deep Web, although he gets there through the bank's home page, which is on the regular web.[23]

---

20 Mitch Waldrop, *DARPA and the Internet Revolution: 50 Years of Bridging the Gap* (Defense Advanced Research Projects Agency, 2018).

21 Vincenzo Ciancaglini, Marco Balduzzi, Robert McArdle, and Martin Rösler, "The Deep Web," *Trend Micro*, 2015.

22 Lucas D. Introna and Hellen Nissenbaum, "Shaping the Web: Why the Politics of Search Engines Matters," *Information Society* 16, no. 3 (2000):169–185; Eszter Hargittai, "The Social, Political, Economic and Cultural Dimensions of Search Engines: An introduction," *Journal of Computer-Mediated Communication* 12, no. 3 (2007): 769–777.

23 Hurlburt, "Shining Light on the Dark Web," pp. 100–105.

The Darknet or Dark Web is part of the Deep Web, and, in fact, it is its most deeply concealed layer.[24] Users can only visit it by means of a special browser or using special network protocol definitions, so that most actions taken on it are completely anonymous. The unique features of the Dark Web, compared to the Deep Web, are the special protocols (rules) and the special infrastructure required in order to access and use it. The special infrastructure sometimes comes in the form of browsers that are programmed to access various protocols, such as Onion, Riffle, Freenet or i2p addresses and more, or as specific network definitions known only to authorized users.[25] Organizations, such as the military, intelligence, and the police and even businesses and a few individuals can set up Dark Webs, whose protocols and browsers will be unique and known only to their owners.[26]

The most widespread Dark Web is the Onion Route (TOR), which had been developed by US Navy laboratories to facilitate private anonymous communication between intelligence agents and was exposed in 2002. This network consists of thousands of internet sites that can only be accessed using the TOR browser. These sites are called "onion" sites after the onion suffix in their names and the onion image, which acts as a metaphor for the many layers hampering access to the core. Onion sites are not catalogued and no general browser can effectively find them. TOR operates in a way that communication between two points (e.g., the user's computer and the site the users wants to visit) is not transmitted directly but rather through several intermediate stations (IP addresses). Each station receives a unique means of decoding, only knows the next station in the chain, and does not know the final station or the source. The reason is that many of the servers are encrypted, so that the internet provider is able, in most cases, to discover the first node reached by the user but not the subsequent nodes.[27] The server receiving the call is also unable to locate any other nodes, apart from the

24 Gabriel Weimann, "Going Darker: The Challenge of Dark Net Terrorism," *Wilson Center*, April 27, 2018.

25 Dakota S. Rudesill, James Caverlee and Daniel Sui, *The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box,* Ohio State Public Law Working Paper no. 314 (Ohio State University, Woodrow Wilson International Center for Scholars, 2015).

26 Ibid; Lev Topor, "Deep and Dark Webs – Liberty or Abuse," *International Journal of Cyber Warfare and Terrorism* 9, no. 2 (2019): 1–14.

27 Roi Goldschmidt, "Use of Anonymous Communications Networks on the Network for Criminal Purposes," Knesset Research & Information Center, January 2012 [in Hebrew].

node from which it receives the call for information/ interaction. In fact, this node also changes every few minutes. In this way, all the nodes are on a route that is protected in most cases from private or government surveillance.[28]

The main problem with TOR lies in its unique nature: It allows security and anonymity, but it is not hidden from the local network providers. Although they cannot discover the information and the destinations of network users, such as of western intelligence operatives in hostile countries, this problem can be solved by elimination, at least partially: Local network providers can discover that among a number of users in a specific neighborhood, for example, one or more users have unusual network traffic. In this way, the authorities can only see normal network traffic, and not see private and anonymous web surfing.[29]

Besides the special network traffic of the Dark Web, which, as stated, creates a confusing, hard to locate trail of several nodes, the TOR platform, in the form of an easy to use browser, can stop sites from gathering information about users. Privacy is sacred on the TOR network, and no site on it can collect information about location, types of hardware, software, or patterns of use. With the TOR browser, it is also possible to eliminate the use of JavaScript, HTML 5, media, images, icons, symbols and more. Thus, the Dark Web creates an interesting paradox: On one hand, it sanctifies privacy and anonymity, and on the other hand, it is used by criminals, terrorists and other hostile elements, who can trade information with a low signature.[30]

In addition, the Dark Web is a kind of marketplace for illegal activities, such as trading in cyber tools. For example, if a company wants to cause damage to a competitor, it can enter the Dark Web, buy an attack with ransomware, malware, or spyware, or activate a bot network or any other tool. In most cases, buyer and seller conduct the transaction with bitcoins, to maintain anonymity. The Dark Web also is used for trading in weapons and drugs and for distributing pornographic material.[31] Terror organizations can find it very convenient for their activities: For about a decade, much of the communication between the leaders of al-Qaeda all over the world took

28 Eric Jardine, *The Dark Web Dilemma: Tor, Anonymity and Online Policing* (London: Global Commission on Internet Governance and Chatham House, 2015).
29 Topor, "Deep and Dark Webs – Liberty or Abuse."
30 Ibid.
31 Nyshka Chandran, "From Drugs to Killers: Exploring the Deep Web," *CNBC,* June 23, 2015; Cara McGoogan, "Dark Web Browser Tor Is Overwhelmingly Used for Crime, Says Study," *Telegraph,* February 2, 2016.

place on the Dark Web.[32] But the Dark Web also hosts entities working to foil terror attacks, such as internal security and intelligence organizations.[33] According to data from Webhose, about fifty percent of activity on the Dark Web is criminal in nature, which means that the other fifty percent is legal and legitimate.

Today, the Dark Web is increasingly being used as a tool for activists to organize protests against totalitarian regimes. It also hosts sites that mirror well-known internet sites, such as those providing news and information from the West, which can be accessed by people living under totalitarian restrictions. For example, the address facebookcorewwwi.onion leads to the "onion version" of the social network for users in countries where Facebook is blocked. Similarly, nytimes3xbfgragh.onion leads to the "onion version" of the *New York Times*. In November 2018 a former engineer from Facebook uploaded an "onion version" of Wikipedia—a Dark Web mirror version of the free encyclopedia, which is completely or partially blocked in various countries.[34] While totalitarian regimes deal with the problem of anonymity by means of arrests and interrogations, the US administration chose to flood the world with TOR, calling for the promotion of freedom of speech, human rights, anonymity, free and open communication, and opposition to all totalitarian regimes.

Potential Uses of the Dark Web for Influence Campaigns

Previously, when a power wished to influence another player in the global arena—a country, terror organization or specific individual—it made use of military or economic power. The cyber era has added a new dimension to the concept of "power," incorporating advanced cybernetic capabilities that are easy to operate and can overturn the traditional balance of power and even serve as "tie breakers." For example, a country might develop a secret military project that could be destroyed if cyber criminals leak the details on the web.[35] In July 2018, it emerged that an American hacker had

32 Weimann, "Going Darker."
33 Topor, "Deep and Dark Webs – Liberty or Abuse."
34 Amitai Ziv, "The Dark Side of the Internet: Drugs, Weapons, Cyber Attacks and Regime Opponents," *TheMarker*, July 18, 2018 [in Hebrew].
35 Joseph S. Nye. "Soft Power and American Foreign Policy," *Political Science Quarterly* 119, no. 2 (2004): 255–270; Ernest J. Wilson, "Hard Power, Soft Power, Smart Power," *Annals of the American Academy of Political and Social Science* 616, no. 1 (2008): 110–124.

tried to sell on the Dark Web the plans for sensitive military drones called MQ-9.[36] In the second trimester of 2019, a company in the military industry contacted one of the writers of this article with a request to locate a leak about it on the Dark Web, due to its concerns over the leak of sensitive plans by some of its employees.

Some of the Dark Web platforms that could be used for influence campaigns include leak platforms; passive data storage platforms; and trading platforms, which include offers of selling information, cyberattack tools and bots, as well as fake "involvement" in social networks.

Leak Platforms

In an age when it is possible to steal over a terabyte of data in a fraction of a second on a mobile storage device and to leak information from government, security, and business meetings anonymously in real time, it is not surprising that the frequency of leaks is increasing.[37] Leaks are often used by people opposed to controversial actions, particularly on matters relating to the military and security. At the same time, the local government can be the source of the leaks, either directly or through deception: Just as security forces and the police use agents who operate on the Dark Web (and the regular internet) or who pose as minors to trap pedophiles, intelligence organizations all over the world use the leak platforms by spreading a kind of "appeal" for leaks and offering payment in return. Moreover, many governments contact external suppliers, such as business intelligence companies or high tech companies in order to monitor, analyze, and operate certain elements on the Dark Web.[38] In this context, the Dark Web project can also be a large honey trap.[39]

Another obvious example of a leak platform is the free press website Wikileaks, which was set up in 2006 and since then has caused several media controversies after leaking hundreds of thousands of documents, items of information, and other material about contentious American activity. The site is located on the regular internet but recommends that users who wish to share leaked information resort to the Dark Web. They are referred to a link where they are asked to enter the details of the information and upload any

36 Ziv, "The Dark Side of the Internet."
37 Scott Shane, "The Age of Big Leaks," *New York Times*, February 2, 2019.
38 Chris Bing, "How the FBI Relies on Dark Web Intel Firms as Frontline Investigators," *Cyber Scoop*, April 13, 2017.
39 Topor, "Deep and Dark Webs – Liberty or Abuse."

supporting files, such as pictures or documents, although the site is under no obligation to verify the report.[40] Another leak platform is the Secure Drop system, which the Freedom of the Press Foundation developed and promotes. It provides media services and anonymous encrypted transfer of data. Press syndicates such as Associated Press, the Guardian, New York Times, Al Jazeera, and many others, use this system to share sensitive information.

Governments can use both the above platforms to leak information if they feel its publication on traditional media could be harmful. A prominent example was the information about the nuclear weapons held by Israel. Israel has not signed the international Non-Proliferation Treaty (NPT) on nuclear weapons, so any overt publication about its weapons could be problematic in terms of international law. At the same time, an anonymously initiated publicizing of an arsenal of strategic weapons could strengthen Israel's geopolitical status and serve as a signal to hostile countries. Thus, for example, there is a famous dedicated page on the Hidden Wiki site with information about the Israeli nuclear program, including its timeline, doctrine, policy, and methods of implementation. More about the Israeli nuclear program, as well as the Indian program and other controversial projects can be found in other Dark Web forums.

Passive Platforms for Data Storage

These are sites or forums for discussions where data is shared and stored. For example, leaked files can be uploaded to the DOXBIN site and saved until needed. On May 30, 2019, contact details of thirty employees of the FBI, including home addresses, telephone numbers, emails, family members, and so on were leaked from this site.

Other platforms where information (whether leaked or not) can be stored and discussed include the IntelExchange forum and the Stock Insider, where users who have been approved share information about trading on various stock exchanges and reveal speculative activity. Storage sites are not only used by malicious leakers but often also by government entities and intelligence organizations that wish to share information anonymously. They "stick" the files they want to share onto the storage sites, using a misleading name, and

40 David Leigh, Luke Harding, and Charles Arthur, *Wikileaks: Inside Julian Assange's War on Secrecy* (New York: Public Affairs, 2011).

then send a message to the traditional media (such as by a text message) using the same name.

Trading Platforms

Several anonymous sites offer to buy or sell classified information. Businesses often post requests for leaks about their competitors' activities, and there have been cases where journalists and intelligence personnel have offered to trade information. One such site is SellFile, where information and services are offered for sale with payment by bitcoin. In the case of influence campaigns, it is possible to purchase entire voter lists on the Dark Web, including contact details, as well as political inclinations. With this data, it is possible to target potential voters on social networks.

Not only information is traded on these platforms. Recently published research indicates that the Dark Web is becoming the main source for the sale and delivery of malware designed to infiltrate specific organizations and industrial sectors.[41] This malware may also be used in cyberattacks aimed at interfering with elections. Senior personnel in the US intelligence services estimate that it is highly probable that hackers will try to corrupt or even destroy databases holding voter registration details for the 2020 presidential elections by using ransomware. These kind of cyberattacks generally lock down the infected computers until a ransom is paid, usually in crypto currency. One example is the 2017 global cyberattack, NotPetya, attributed to Russia. The attack used ransomware to screen a technique of data deletion, which made the victims' computers completely unusable. This threat is particularly worrisome in view of its potential influence on voting outcomes. An attack of this kind, if not identified before the elections, could sabotage voting lists, cause enormous confusion and delays, deny many people the right to vote, and even raise questions regarding the validity of the results.[42]

Digital weapons, including malicious software such as EternalBlue and WannaCry—whose tracks lead to North Korea and have caused damage estimated at almost four billion dollars to business and government computer

41 Yossi Hatouni, "What Are the Most Popular Hacking Tools Offered for Sale on the DarkNet?," *People and Computers*, July 11, 2019 [in Hebrew].

42 Christopher Bing, "Exclusive: U.S. Officials Fear Ransomware Attack against 2020 Election," *Reuters,* August 26, 2019.

systems in several countries—are also available on the Dark Web at relatively low cost and could be used by hostile elements for cyber influence campaigns.[43]

In addition to malware and hacking tools, the large number of abandoned accounts on social media platforms are also an important and convenient target for hackers due to their many points of security vulnerability. Bot networks on Twitter, Facebook, and Instagram, designed to spread disinformation and increase "involvement"—by using shares and likes in order to create a misleading impression of public interest around certain content—are offered for sale on the Dark Web for very small amounts. Similar offers are made for separate packages of retweets, likes, and YouTube views.[44]

The three platforms surveyed above have three common uses: to increase the power of the leaking country, to damage the subject of the leaks, and to promote human rights in certain countries. Thus, the РосПравосудие site on the Dark Web has published about fifty million documents dealing with the Russian legal system, with personal details of judges, lawyers, prosecutors, and so on. The operators of the site claim that they are leaking the information as a means of exerting pressure on those who manipulate the law in favor of the regime, and—more importantly—to discredit those who participate in show trials with predetermined outcomes. At present, it is not clear who is behind this site—internal and external elements who seek to undermine Russia's status, or Russian citizens who understand the importance of a proper legal system.[45]

There are numerous examples of how the Dark Web has been used to influence elections. In 2016 the servers of the US Election Assistance Commission were hacked and stolen entry passes of its employees were discovered on the Dark Web.[46] That same year, Russian hackers invested about 95,000 dollars in cryptic currency to set up fake websites and social media accounts to be used for influence campaigns.[47] In early 2017, the US Justice Department revealed that in the framework of attempts to influence the 2016 presidential elections, Russian hackers had obtained access to

43 Ibid.
44 Dan Patterson, "The Dark Web Is Where Hackers Buy the Tools to Subvert Elections," *CBS News,* September 26, 2018; "Influence for Sale: Bot Shopping on the Darknet," *DFRLab*, June 19, 2017.
45 Topor, "Deep and Dark Webs – Liberty or Abuse."
46 Joseph Menn, "U.S. Election Agency Breached by Hackers after November Vote," *Reuters*, December 16, 2016.
47 Topor, "Deep and Dark Webs – Liberty or Abuse."

more than half a billion email accounts on the Yahoo site. The hackers also managed to break into 6,500 user accounts, including some who were targeted in advance by the Russian government, such as journalists and members of the opposition. Access to other accounts was auctioned on the Dark Web, apparently in order to increase the profit from hacking.[48] In 2017, about forty million records of American citizens were offered for sale on the Dark Web for only four dollars. The small amount requested reinforces the belief that the sale was not done for profit but rather for ideological reasons. Furthermore, within the context of the US mid-term elections at the end of 2018, a database of tens of millions of American voters was discovered for sale on the Dark Web. In addition to the voters' personal details, the database also contained information about their political views and which candidates they supported.[49]

These databases can be used to increase the accuracy of targeting potential population groups and the frequency of phishing attacks. In this context, attackers disguise themselves as service providers, such as banks, operating systems, or government institutions, in order to obtain personal details for use in influence campaigns.[50]

Prior to the 2019 elections in Israel, cyber tools were offered for sale on the Dark Web, which apparently had been developed by Ukrainian hackers and were designed to overcome the restrictions imposed by WhatsApp on the number of contacts who could receive messages simultaneously. The tools gave their owner the ability to take remote control of WhatsApp groups in Israel and plant video and text content. In addition, members of the chat group would receive the message from one of the other members of the group, suggesting that the message appeared trustworthy.[51] According to Ben Caspit, Israeli entities recently purchased for hundreds of thousands of dollars the option to send 15 million WhatsApp messages within 48 hours. The ability of Facebook to block this capability is limited, although hackers on the Dark Web will sell a counter defense, which attacks these messages

48 Ilan Geller, "Simple and Brilliant: How Russian Hackers Broke into Millions of Email Accounts without a Password," *Walla*, March 19, 2017 [in Hebrew].

49 Rafaella Geuchman, "Details of 62 Million American Voters Offered for Sale on the Darknet," *TheMarker*, November 6, 2018 [in Hebrew].

50 Patterson, "The Dark Web is Where Hackers Buy the Tools to Subvert Elections."

51 Ben Caspit, "The Threat to These Fateful Elections Comes from the Underworld of the Internet," *Maariv*, September 9, 2019 [in Hebrew].

as soon as they appear and creates enormous artificial demand that causes the system to collapse.[52]

Conclusion

The aim of this article was to draw attention to the Dark Web as an additional channel for implementing cyberattacks and influence campaigns and to explain how the various players achieve their aims. The importance of the Dark Web as a platform for attempts to influence election campaigns has increased in parallel to the growing number of revelations about foreign interference in the elections of various countries, and especially with Russian involvement. Naturally, this has led to a rise in the attempts of governments and media giants to protect themselves against the known techniques of these efforts. In this context, the use of bots to influence social media has perceivably dropped while activity on instant messaging applications has increased. There is also a significant rise in activity on the Dark Web, which provides greater privacy and anonymity than the regular internet, and, as a result, exposing and fighting its influence campaigns therefore presents a greater challenge. Apart from the technological challenge, there is also a conflict between the need to protect public discourse and to maintain the principle of free speech, which the Dark Web aims to promote.

This article surveyed the three main types of leak platforms on the Dark Web: platforms calling for leaks of information, such as WikiLeaks or Secure Drop; passive platforms, such as IntelExchange, DOXBIN or the Stock Insider, where leaked data is stored; and trading platforms, such as SellFile, which offer information for sale and receive requests for information. Malware, spyware, bot networks, and cyber and media encryption tools all can be acquired on the Dark Web for using in influence campaigns, which can be done easily and anonymously.

These tools and the three platforms described are being used by countries and organizations to exercise influence in cyberspace, as shown in the above examples. Although the reliability of the information flowing over the Dark Web is controversial, this is often irrelevant to the entities seeking to influence how people vote; the mere fact of the leak serves their main purpose—to sow doubt and undermine the existing order. Given the relatively low cost of the capabilities offered for sale on the Dark Web and the difficulty of

52 Ibid.

tracking the source of leaks, we can expect a growth of both supply and demand for these tools.

The presence of democratic regimes on the Dark Web and how they use it is another interesting issue. On one hand, they have to deal with the subversive activities of terrorist organizations and totalitarian regimes, as well as with crime, which means there is no alternative to being involved in the Dark Web, as a "know your enemy" tactic. On the other hand, the use that democratic regimes make of the anonymity of the Dark Web appears problematic: Democratic regimes are not exempt from the tough international game, but the methods they use are important, particularly when they claim to be more "ethical." It can be assumed that the democratic administration that launched the Dark Web also makes the most extensive use of it, as a senior US official hinted to one of the authors at a conference in Washington DC in September 2019.

Another ethical question raised here is whether democratic governments confine their use of the Dark Web to actions against their international enemies, or do they also target rivals at home? Members of parliaments all over the world, including members of the Israeli Knesset, leak information from meetings and sometimes face charges for doing so. On the other hand, leaking on the Dark Web offers far greater anonymity, as well as the ability to cause chaos in the political system.