Next Generation Information Warfare: Rationales, Scenarios, Threats, and Open Issues

Roberto Di Pietro, Maurantonio Caprolu, and Simone Raponi

Hamad Bin Khalifa University (HBKU) - College of Science and Engineering (CSE)
Division of Information and Computing Technology (ICT)
Doha, Qatar
{rdipietro, mcaprolu, sraponi}@hbku.edu.qa

Abstract. The technological advances made in the last twenty years radically changed our society, improving our lifestyle in almost any aspect of everyday life. This change directly affects human habits, transforming the way people share information and knowledge. The exponential technological advancement, together with the related information deluge, are also radically changing Information Warfare and its scenarios. Indeed, the consequent increase of the digital attack surface poses new challenges and threats for both personal and national security.
In this paper we discuss the motivations behind the need to redefine the Information Warfare according to its new dimensions. Then, we analyze the potential impact of the new threats on the most sensitive targets exposed by every nation: the Society, the Economy, and the Critical Infrastructures. Finally, for every considered scenario, we analyze existing state-of-the-art countermeasures, highlighting open issues and suggesting possible new defensive techniques.

Keywords: Information Warfare · Critical Infrastructure · Fabric of Society.

1 Introduction

Information has always played a decisive role in both the wars and the revolutions of the past. The knowledge in advance of a particular move of the adversary could completely overturn the fate of a conflict. In fact, the opponent could be militarily more advanced, but knowing which target he intends to hit gives the defender a significant advantage. At this point, it should not come as a surprise to know that a crucial phase of the war is being fought from the information perspective. Information trusted by a target may be subject to manipulation, without the target's awareness. Thus, making decisions based on this counterfeit

This is a personal copy of the authors. Not for redistribution. The final version of the paper is available in the proceedings of the 5th International Conference on Information Systems Security and Privacy (ICISP) 2019, at the link: https://link.springer.com/chapter/10.1007/978-3-030-49443-8_2, with the DOI: https://doi.org/10.1007/978-3-030-49443-8_2

information is absolutely against the interests of the victim, that becomes like a puppet at the mercy of the attacker. The manipulation of trusted information takes the name of Information Warfare.

Over the years, we have witnessed an evolution in the transmission of information, starting from the simple chat to the market up to the current Social Media technologies. One of the first revolutions in the field of information transmission was the optical telegraph, invented by Claude Chappe in 1793, at the height of the French revolution. The device was used to connect, in real time, the military bases of Lille and Paris. About 60 years later, in 1854, Antonio Meucci invented the telephone, with which it was possible to overcome many of the limits of the telegraph system. The telephone was based on the transmission of the voice, and therefore it was not limited to the transmission of written documents. Half a century later, in 1895, Guglielmo Marconi had the intuition that radio waves could be used for wireless communications, giving rise to wireless telegraphy via radio waves. The invention of the radio revolutionized the communication systems in force at the time and led to the development of radio communication methods used even today. Many years later, in 1958, General Dwight David Eisenhower created the Advanced Research Projects Agency (ARPA) as a direct response to the Russian launch of Sputnik. The aim of the ARPA project was to provide the United States with a technological advantage over other countries. The project gave birth to Arpanet, a network that linked the supercomputers of the various research centers, and which laid the foundations of the modern Internet. The advent of the Internet has led communication distances to be filled as never before in history, completely revolutionizing the information communication ecosystem. The related introduction of web pages, forums, and Social Media has radically changed many aspects of users' lives from a social point of view, leading to a new logic of information that prefers speed and immediacy to accuracy and reliability. The information during the sharing process undergoes adjustments, enrichments, researching active participation by a dynamic audience until it becomes a heterogeneous collage, from which the original source and opinion can hardly be extracted. People, and Society with them, are not the only potential victims of Information Warfare.

Contribution. In this paper, we first discuss the motivations that lead to redefining the concept of Information Warfare, consequently to the appearance of its new dimensions caused by the advent of new technologies. Each section represents a typical target of the Information Warfare, regarding aspects of the society, the economy, and the Critical Infrastructures of a generic Nation, respectively. For every considered aspect, we build one or more plausible detailed real-world scenarios, showing from which possible threats could be threatened. For each threat, we identified the current state of the art, both in terms of attacks and defenses. In addition, we identified open problems that still affect these fields and the countermeasures that can be implemented, to ensure that readers can have a starting point to enrich the state of the art with innovative and prestigious solutions.

Roadmap. The paper is organized as follows. Section 2 resumes the motivations behind the introduction of the Next Generation of Information Warfare. Sections 3, 4, and 5 introduce innovative scenarios with associated threats, study of the state of the art and open problems, and proposals of countermeasures related to Fabric of Society, Cryptocurrencies, and Critical Infrastructure, respectively. Finally, Section 6 draws some concluding remarks.

2 The Need for a Next Generation of Information Warfare

Over the years, new technologies have continually changed society with new discoveries and inventions able to improve human life. The progress machine tirelessly introduces tools and resources that facilitate everyday tasks, since the dawn of humanity.

Usually, processes that radically change the human lifestyle are gradual and take time to complete the revolution. In the past few years, modern technology has made a fast and radical change of our society, modifying our habits with many functional and utility devices like smartphone, smartwatch, and other smart devices, making our lives faster, easier, and funnier. Technology is raising new kinds of habits and addictions, changing every aspect of our society such as personal interactions, education, communication, financial services, entertainment, to name a few, with a wild race to the digitization of information of all kinds, from the most sensitive to the most (apparently) harmless.

Nowadays, almost all our daily activities are held using digital devices, that offer us a huge number of different web-based services through which we manage every aspect of our lives. These services help us to learn, have fun, pay bills and manage our bank accounts, communicate with distant friends and meet with new ones, handle personal agenda, buy items and services, and so on. Such technologies, on one hand, guarantee access to a boundless range of services and information to anyone, on the other hand, allow service providers to access an equally boundless quantity of users' personal information, often harvested without the users knowledge. Moreover, using online services like Social Media, users voluntary publicly share private information like their personal data, family relations, private multimedia contents, thoughts and experiences, and many others that allow everyone to know a person without ever meeting her. In the era where the wealth is given by information, online Social Media represent real gold mines, in which even without a license anyone can go picketing. Such kind of information represents a big opportunity for different entities such as governments and advertising companies, opening scenarios that would have been unimaginable just a few years ago.

This frenetic technological advancement radically changed Information Warfare scenarios, posing new threats for personal and national security that every nation must take into consideration to safeguard its own security against malicious actors.

The existing contributes related to Information Warfare usually deal with the subject by categorizing the arguments based on the "warfare capabilities and directions" of the most powerful nations (USA, Russia, China, others) or based on the pillars of Information Warfare: Psychological operations (PSYOPS), Military Deception, Electronic Warfare, Physical destruction, and Operational Security (OPSEC). Unlike these approaches, we will discuss new threats never addressed before in the literature, categorizing them into several macro areas representing the attack surface of a generic nation. Every threat is inserted in a real case scenario and explained in details with their threats and possible impacts. For every scenario, we will also highlight open issues, raising problems that need to be addressed in order to mitigate security threats derived from the technological advance happened in the past few years. Our aim is to spread these new threats with their respective state of the art and existing countermeasures to the community of researcher in the cyber-security field, suggesting also new possible ones when not sufficiently covered in the literature.

3 Fabric of Society

The introduction of new technologies, such as Social Media, Social Networks, Media Sharing services, online forums, and online instant messaging services, make information sharing and propagation extremely fast. The number of Internet users, together with the amount of available information, is growing continuously from day to day. In 2014 there were 3,079 billion Internet users, a number that has grown in the following years up to 4,346 billion Internet users in March 2019 [5]. The number of Internet users has increased by 41.15% in less than five years, leading to a consequent increase in contributions on the web. As an example, Google's search in 2016 knows about over 130 trillion pages [3], but this is only the tip of the iceberg. The Deep Web, also called the hidden or invisible web, represents the part of the World Wide Web whose contents are not indexed by common web search engines, and is estimated to be 500 times the size of the indexed web [2], also known as Surface Web.

People, while surfing the web, have at their disposal this almost infinite amount of information, some truthful, others not. As a consequence, the ideas of individuals are no longer built autonomously (i.e., based on facts obtained independently), but based on hundreds of thousands of opinions read on the web, of which only a negligible part is authoritative. In this way, shifting the attention of the masses and changing individuals' opinion is a breeze, in the first case to make events of national importance go unnoticed, in the other one, to set the agenda. Disinformation grows in step with information, making it difficult to distinguish reliable information from unreliable ones. In addition, people do not use to double check the content found on the web, due to either lack of time or will, resulting in an unintended spread of unreliable information that bounds around the web.

To make matters worse, the concept of the filter bubble comes into play. The filter bubble describes the tendency of social networks such as Facebook and Twitter to lock users into personalized feedback loops, each social network with its own news sources, cultural touchstones, and political inclinations [4]. Users surfing the web will be overwhelmed by a wave of personalized content, based on previous knowledge of their interests, their location, and their browsing history. This phenomenon tends to eventually lower the critical spirit of individuals, placing them in front of a vision of the personalized world, that absolutely does not reflect reality.

In this section, we describe how the Information Warfare could threaten the Fabric of Society, for instance by piloting the elections in democratic states, by running disinformation campaigns to cause unrest and discredit people or governments, and by indoctrinating the population resident in states with Authoritarian governments.

3.1 Scenario: Democratic Election in a Country

In this scenario, we will take into account the political election of a democratic Country. The state promotes transparency and fairness in elections, providing the candidates with a fair media space and controlling their advertising according to principles of equality and correctness. According to the definition of the former U.S. ambassador to the United Nations, “Democratic elections are not merely symbolic. They are competitive, periodic, inclusive, definitive elections in which the chief decision-makers in a government are selected by citizens who enjoy broad freedom to criticize the government, to publish their criticism and to present alternatives [21]. Democratic elections are competitive, because the mere right to participate in the ballot is not enough. Indeed, political (and not political) groups involved in the elections must guarantee fairness, by avoiding censorship and respecting the rules. Both opposition parties and candidates must enjoy the freedom of speech, as well as bringing alternative policies and candidates to the voters. Democratic elections are also definitive, because they determine the leadership of the government. The party leader work has the burden of leading the country, promoting the political program they proposed during the election campaign.

Threat: Inference in Political Election
Political elections within a country are not only reflected in the interests of citizens. Companies and institutions (either local or foreign) may have an interest in illegally interfering with the electoral campaign, with the aim of piloting thus obtaining profits in the short, medium, or long term. Companies and institutions, especially Governments, could use Social Media to profile users and manipulate their attitudes and behaviors through the use of hate speech, fake news, and manipulative campaigns. This user profiling allows companies and institutions to build targeted (possibly fake) advertising, with the aim of manipulating the vote of individuals.

In recent years, several works concerning the interference of bots and actors in the political events have been proposed. In [31], E. Ferrara provided an extensive statistical analysis of the Macron-Leaks disinformation campaign that occurred during the run up to the 2017 French presidential election. A similar study, but on another target, was carried out by Forelle et al, in [33]. The authors study the role of social and political bots in Venezuelan political conversations, together with the relative conditioning of the public opinion. They pointed out that these automatic scripts generated content through Social media platforms, interacting with people, and that most of the active bots have been adopted by Venezuela's radical opposition. Hegelich et al., in [40], investigated whether bots on Twitter have been used as political actors during the conflict between Russia and Ukraine. They pointed out that bots exhibit three distinctive patterns of behaviors: (i) trying to hide their identity, (ii) promoting topics through the use of hashtags, and (iii) retweeting selected tweets and messages. K. Starbird in [70] explored the alternative media ecosystem through the Twitter's magnifying glass. The findings describe a subsection of the emerging alternative media ecosystem and provide insights on how websites that promote conspiracy theories and pseudo-science may function to conduct underlying political agendas. In the primary work [45], Howard et al. studied the use of political bots during the U.K. referendum on EU membership. The authors discovered that political bots had a small but strategic role in the referendum conversation.

In this threat, some of the crucial open problems concern: (i) the detention of illegal political disinformation campaigns, (ii) the reaction after the identification of an illegal disinformation campaign, and (iii) the understanding of the extension of the bots network. The possible countermeasures should take into account the freedom of speech of individuals. Indeed, adopting measures that involve some kinds of censorship would apparently solve the problem, but it would also deprive users of the possibility of expressing their opinion, thus impoverishing the diversity of thought.
Intelligent agents, the result of the artificial intelligence state of the art, could be trained in recognizing both targeted political advertisements and political fake news, with the aim of obscuring the view to the user while navigating a social network, thus safeguarding the user's political opinions. Other agents could be used to analyze in detail the relationship graph, with the aim of isolating content proposed by members of cliques in the graph. Recall that a clique in the graph represents a complete subgraph, i.e., each node in the subgraph is connected through an edge to all the other nodes of the subgraph itself. Bots and misinformers tend to have a high number of contacts, in order to efficiently spread their message, in such a way that it impacts a greater number of people at the first step of communication. After that, each bot, in addition to creating and disseminating its contents, will work to share the information of the other allied bots in order to reach even more viewer. To do this efficiently, the only users in common between two bots should be the bots themselves, and the catchment area reached would be increased with minimal effort and resources. To understand the extent of the bot network there is the need to distinguish bots from normal users. One of the first steps was taken by Chu et al. in [19]. To assist human users in identifying who they are interacting with, the authors focused on the classifi-

cation of humans, bots, and cyborgs accounts on Twitter. During the study, the considered respectively legitimate bots (i.e., bots that generate a large number of benign tweets delivering news and updating feeds), malicious bots (i.e., bots that spread spam or malicious contents), and cyborgs, that can be either bot-assisted human or human-assisted bot. In [61], the authors studied astroturf political campaigns on microblogging platforms. They represent politically-motivated individuals and organizations that use multiple centrally-controlled accounts to create the appearance of widespread support for a candidate or opinion. The study led to the implementation of a machine learning framework for Twitter, that detects the early stages of the political misinformation viral spreading by combining topological, content-based, and crowd-sourced featured information diffusion networks.

3.2 Scenario: Freedom of Information

This scenario takes into account a State that does not make use of censorship techniques to silence the citizens. People are allowed to publicly express their opinion, in traditional ways as well as with modern means, such as online social networks, blogs, forums, and possibly others. The social platforms do not incur in traffic filtering techniques, that are usually applied to deny access to specific websites, allowing users to freely adopt any communication service like real-time messaging applications and mail services. Moreover, the government has no control over the content of the transmitted and received information, thus allowing users to express their opinion without being incurred in fines or punishments. Citizens are free to express both their thoughts and their opinion about any topic, whatever they are. The information conveying through social media can be of any kind: true or false, trusted or not trusted, accurate or not accurate.

Threat: Disinformation campaign

One of the first documented examples of supposed Fake news takes us to Ancient Rome in July 64 b.C. The emperor Nero set fire to an entire district of the city to make room for new buildings, accusing the Christian community of the Crime. He created a fake news artfully both to not turn the public opinion against himself, and to continue his persecution campaign against the Christian community. Going forward over the years other famous examples can be found. In 1933, the palace of the Reichstag, seat of the German parliament, was set on fire. The leaders of the Nazi party took advantage of the opportunity to blame the opponents of the Communist party, gaining consensus that led to their final rise to power. These two cases make us reflect on the fact that the invention of news or the alteration of partially true ones makes it possible to maneuver the public opinion, obtaining illicit advantages. The same principle still applies nowadays, with a sounding board that has never been so wide due to the speed of social media information propagation. The study from researchers at Ohio State University finds that fake news probably played a significant role in depressing Hillary Clinton's support on Election Day. The study offers a first look at how fake news affected voters choices, pointing out that about 4% of President Barack Obama's 2012 supporters were dissuaded from voting for Clinton in 2016 because of fake news stories [9]. The lack of truthfulness of information makes the detection of the trustworthiness of content hard for citizens, creating doubts and confusion among the population. Artfully built news usually have mixed with any size fragments of truth over time, escaping the control of the creator, who usually manages to govern the spreading only for a short time. These news then assume realistic contours, becoming in effect truthful news (as accepted by all as such), ignoring denials or not granting replication rights. Foreign governments, as well as terrorist groups and activists, could exploit these uncertainties on Social media to undertake several kinds of disinformation campaigns, to undermine the credibility of the state or to control public opinions, with the aim of generating chaos and destabilizing the population. In the course of history there have been numerous cases in which the use of disinformation campaigns has caused discontent among the population, disagreements, and revolts, giving the history a presumed truth, impossible to ascertain.

There is more information being shared than ever before, and ordinary citizens are playing an active role in the news ecosystem. Among them, there are users that use to run provocative posting intended to produce a large volume of inflammatory and digressive responses, they are called "trolls". Over the past years, trolls played as state-sponsored actors, with the aim of manipulating public opinion on the web, often around major political events. Although the trolls are often involved in spreading disinformation on Social Media, there is still little understanding of how they operate. In [76], the authors proposed a study with the purpose of understanding better the content dissemination and its influence on the information ecosystem. In [50] the authors studied the sockpuppets, i.e., users that create multiple identities and engage in undesired behavior by deceiving other or manipulating discussions. In this work, the authors showed how the sockpuppets differ from ordinary users in term of their posting behavior, linguistic traits, and social network structure.

Trolls are changing the Internet personality. What trolls do to laugh, provoke, and upset, ranges from clever pranks to harassment up to violent threats. Doxxing –publishing personal data, such as social security numbers and bank accounts– and swatting, calling in an emergency to a victims house so the SWAT team busts in, are just two common practices of these individuals. Trolls are turning social media and comment boards into a giant locker room in a teen movie, with towel-snapping racial epithets and misogyny [8]. As if it were not enough, trolls play the role of disinformation diffusers, with the sole purpose of directing the attention of the masses elsewhere and conditioning their judgment. How could these users who, by leveraging their freedom of expression, dangerously influence people's opinions, be stopped? How is it possible to recognize them? How is it possible to protect users from the toxic behavior of other users? Would it be morally right to put them in an Internet quarantine? Several work have been proposed to face these issues. In [32], A. Fokin emphasized the role of hybrid warfare respect to Information Warfare, with a particular focus on the role of hybrid warfare tactics and trolling in Internet media. The author measured how and to what extent certain cyber activities influence the public opinion. The results provided an approach to evaluate the risk potential of trolling and outline recommendations on how to protect the state and society if trolling is used as an instrument of hybrid warfare. The authors in [29] proposed an approach for quantifying the authenticity of online discussions based on the similarity of online social media accounts participating in the discussion, to know abusers and legitimate accounts. The proposed method uses several similarity functions for the analysis and classification of online social media accounts. In [54] the authors discussed the difficulty of recognizing trolls automatically and proposed a pragmatic study. They assume that a user who is called a troll by several people is likely to be one. They experimented with different variations of the definition, and in each case they trained an efficient classifier. Furthermore, there are websites, such as “EU vs Disinfo” [7] that produce weekly disinformation reviews. Their database contains over 3,800 disinformation cases since September 2015 and is the only publicly accessible, international database of disinformation cases.

3.3 Scenario: Authoritarian State

This scenario takes into account a government in an Authoritarian State, that leads the Country without political opponents. In this authoritarian form of government, the power is centralized in a single organ (or in the hands of a single dictator) and is limited neither by constitutions nor by laws. Typically, authoritarian regimes make use of a censorship policy, designed to preserve their political dominance within the State, like North Korea in the past. As a consequence, citizens are not free to talk about political issues conflicting with the ideas of the regime and the main communication channels (such as missives, mail services, messaging apps, even the spoken words) are intercepted, controlled, and censored where necessary. Fundamental rights such as freedom of expression, opinion, and speech, are not guaranteed, allowing the regime to filter contents to make sure to safeguard its own dominance. In this context, the Authoritarian government could take advantage of information control, making use of Social media, forums, blogs, and other communication means, to disseminate information aimed at maintaining political and social supremacy and stability.

Threat: Political Indoctrination of the Population

By controlling and filtering contents in both Social Media and other communication channels, an Authoritarian government is able to control the population by repressing every form of thought contrary to the principles of the dictatorship. The censorship of the conflicting opinions coming from the resident population, together with the filtering of news coming from abroad and the dissemination of appropriately modified contents, makes the population willing to believe that the general situation of the country is flourishing and hard to improve, and that the Government's work is always right and effective. With these assumptions, the population will be unwilling to organize riots or protest actions, blindly trusting the Government, which will continue to cover up and hide the inconvenient truth.

Dictators do not survive because of their use of force or ideology, but because they are able to convince the population, rightly or wrongly, about their competence. The dictator can invest in making convincing state propaganda, censorship independent media, co-opting the elite, or equipping police to repress attempted uprisings. In [38] the authors showed that incompetent dictators can survive as long as economic shocks are not too large, and that repression is used against ordinary citizens only as a last resort when the opportunities to survive through co-optation, censorship, and propaganda are exhausted. In [65] the authors characterize a ruler's decision of whether to censor media reports that convey information to citizens who decide whether to start a revolution. Both the censorship and the propaganda have been studied in several contexts: the authors in [52] studied the censorship and propaganda in the 1991 Gulf War; a similar work has been done in [48] applied to the Canada's Great War, to post-genocide Rwanda [72], to the World War I [35], and to the World War II [43]. The speed of information propagation due to the advent of Social media has allowed dissidents to express their opinion in the face of an ever-increasing public. This enabled the governments of the authoritarian states to adopt more studied and aggressive censorship policies. In [42] the authors claimed that private companies that run Social Media and search engines, despite their free-speech-friendly philosophy, employ terms of service that censor a broad range of constitutionally protected speech. In [44] the authors analyzed in detail the Social Media censorship as well as both the regulations and the new restrictions to protest and dissent. Other work are referred to the Chinese censorship situation: in [14] the authors presented the first large-scale analysis of political content censorship in Social Media, i.e., the active deletion of messages published by individuals, while web articles [11] pointed out how the censorship make the China different from the West, with the list of Social Media that have been replaced by other ones which the government can monitor.

Several technologies have been introduced to allow dissidents to circumvent the censorship imposed by governments. In [23] the authors presented the various techniques and compared the general methods to break through, including Virtual Private Network (VPN), Secure Shell (SSH), IPv6, proxy tools, hosts file modifications, and web proxy. Among the many, two of the most used nowadays are the VPNs and Tor. VPN is a technology that allows safe communication through an encrypted connection over an insecure network, such as the Internet. Applications running across a VPN may therefore benefit from the functionality, security, and management of the private network [53]. In the literature, there are many works that allowed citizens to circumvent censorship policies using VPNs. In [57] the authors worked on VPN Gate. VPN Gate is a public VPN relay service designed to achieve blocking resistance to censorship firewalls such as the Great Firewall (GFW) of China. To achieve such resistance, the authors organized many volunteers to provide a VPN relay service, with many changing IP addresses. In recent years, new technologies such as high-speed Deep Packet Inspection (DPI) and statistical traffic analysis methods had been applied in country-scale censorship and surveillance projects. The traditional encryption solutions do not hide statistical flow properties, and new censoring systems can easily detect and block them “in the dark”. The authors of [73] proposed a novel traffic obfuscation protocol, where client and server communicate on random ports. The result of this research is an open-source VPN tool named GoHop and the development of several obfuscation methods, including pre-shared key encryption, traffic shaping, and random port communication. Tor [24], the acronym of The Onion Routing, is one of the most popular anonymity systems. The main idea is that the user selects a circuit that typically consists of three relays –an entry, a middle, and an exit node. The user negotiates session keys with all the relays and each packet is encrypted multiple times, first with the key shared with the exit node, then with the key shared with the entry node (also known as the guard). To send a packet to the final destination anonymously, the packet is first sent to the guard, which removes the outer encryption layer and it relays the packet to the middle node. In turn, the middle node removes its encryption layer and relays the packet to the exit node. Lastly, the exit node removes the last layer of encryption and relays the packet to its final destination [51]. Although Tor is one of the most widely used tools to circumvent censorship [6], some states have implemented mechanisms either to block it, or to make it complex to interact with the platform [74]. Furthermore, many techniques have been introduced over the years to either partially or completely deanonymize users browsing the Dark Web [51] [67] [15] [71].

4 Cryptocurrencies

Nowadays, more and more nations are thinking about establishing a state cryptocurrency that will support or replace the classic currency. This kind of scenario, on one hand, introduces several advantages of practical nature, such as no longer having to print physical banknotes, no longer need banking institutions that keep track of balances and transactions, faster and (supposed to be) more secure transactions, and so on. On the other hand, it could expose the Nations economy to a new series of cyber-security threats. Indeed, the classical physical currency is vulnerable to several indirect attacks that mainly aim to its devaluation, such as speculative attacks. However, other kinds of attacks such as denial of services are very difficult or not feasible, due to the physical nature of the classical currency. Indeed, an attacker could target the electronic systems that allow virtual transactions, causing a temporary block of this service, but there is no way to stop transactions with cash payments. A cryptocurrency instead, as a virtual asset, is exposed to direct attacks with consequences ranging from blocking the system for a short time to its total destruction. In the first case, malicious entities could prevent legitimate users to join the network, or isolate the peers that validate transactions, leading to the total network paralysis. In this eventuality, no transactions are possible in the network, because users are not able to create them or peers are not able to receive them. If the attacked cryptocurrency is the only currency available in the state, citizens will no longer be able to make transactions of any kind. Consequently, the sale of goods and services among citizens would fall into anarchy, being possible only through the adoption of antiquated forms of exchange such as barter.

4.1 Scenario: Trust in Maths

This scenario takes into account a cryptocurrency that relies on mathematical properties for its protocol security. To guarantee some properties like Confidentiality, Integrity, Authentication, and Availability needed for the security of every communication, the cryptocurrency protocol uses different cryptographic techniques based on mathematical problems. Users trust the system because of the difficulty of the crypto-challenges derived from the aforementioned properties, recognized as computationally hard to solve by the worldwide community.

Threat: Collapse of the Cryptocurrencies foundation

In this scenario, the major threat is represented by an adversary that reduces the mathematical complexity of the problem on which the cryptocurrency relies on, becoming able to solve it in an optimized way. This knowledge makes the adversary capable to control the cryptocurrency network, exploiting its capabilities (that other peers do not have) to perform illicit activities, like the validation of fake transactions. The same result could happen if an adversary discovers a zero-day vulnerability in the implementation of one cryptographic function used by the cryptocurrency's protocol and develop a methodology to exploit it.

Hash functions are the pillars of the most important cryptocurrencies. Bitcoin, for example, relies on hash functions and their pre-image property to ensure the immutability of the ledger. Several attacks against the most important hash function implementation are discussed in the literature as well as against the compression function they used. The most important are the Chabaud and Jouxs attack of SHA-0 [18], and the hash function attack techniques introduced by H. Dobbertin against MD5 [25] [26] [27] [28]. These techniques are not applicable against SHA256 and SHA512, used by Bitcoin and other major cryptocurrencies, as investigated by several researchers in [39] [60] [63].

4.2 Scenario: Trust in the Computational Power

In this scenario, the major concern for cryptocurrency security is represented by an attacker with an unexpected high computational power. Possible threats include Quantum Computing that, even if the research is still in its infancy, may be able to efficiently solve problems which are not practically feasible on classical computers. This scenario takes into account a cryptocurrency that relies on the computational power for its security. This is also the case of Bitcoin, which relies on the computational difficulty of calculating hashes for Proof of Work (PoW) security. The protocol provides users with cryptographic challenges to be solved to validate transactions. Users have to spend a certain amount of resources, like CPU cycles, to solve these challenges. Then, peers need to reach a consensus in order to extend the public ledger of transactions. This means that the security of the network is guaranteed as long as the majority of the computational power is owned by honest nodes. Users trust the system because of the difficulty for a single entity to have the 51% of the whole computational power available in the entire network.

Threat: New technologies
With its huge computational power, a quantum computer could be used to attack cryptocurrencies networks whose security is based on the difficulty for a single entity to hold the majority of the computational power of the entire network. Moreover, if a few single entities control a large part of the total computational power, the risk of joining forces to control the majority cannot be underestimated.

The potential danger posed to IT security by quantum computing was first established in 1994. That year saw the publication of a quantum computer algorithm [68] by the US mathematician and computer scientist Peter W Shor. In his work, he demonstrated how encryption techniques - previously considered secure - could be broken in a matter of seconds by factorization, or reducing a number into its constituent factors. To do so, the Shor algorithm used the computing power of quantum computers [30].

A possible solution for the threats posed by quantum computing and other advances in technologies, is certainly the development of proof of works (or other control protocols) information-theoretically secure. This means that the security of the protocol derives exclusively from Information Theory, rather than depending on other weak assumptions like the computational hardness. In this case, it is impossible for an adversary to break the system, even with unlimited computing power, simply because the attacker does not have enough information to calculate the solution.

Mining pools are a way for cryptocurrencies miners to pool their resources together and share their hashing power while splitting the reward equally according to the number of shares they contributed to solving a block. In some cases, like Bitcoin, very few mining pools control more than the 50% of the total computational power of the network. [1]. In blockchain base systems like cryptocurrencies, game theory can be used to prevents cheating in the network community [16].

4.3 Scenario: Infrastructure

Although anyone can run a cryptocurrency node anywhere on earth, the nodes that compose the network will hardly be physically uniformly distributed around the globe. This means that with high probability most of the nodes are hosted in few Internet Service Providers (ISPs). Consequently, most of the network traffic traverses network devices controlled by these few ISPs. As a direct consequence of this, denial of services attacks could be more easy to perform, by attacking ISPs' infrastructures for indirectly hit the cryptocurrency network availability. Moreover, malicious ISPs could filter the cryptocurrency's network traffic, compromising the overall functionalities or isolating specific nodes.

Threat: Hijacking Cryptocurrency network
In this section, the threats related to directly attack the network infrastructures will be analyzed. Possible threats include denial of service attacks, in the attempt to disrupt cryptocurrency resources denying crypto coin users access. More specific Routing Attacks such as Border Gateway Protocol (BGP) hijacks, can partition a cryptocurrency network into two or more disjoint components. Another threat consists of delay the delivery of a block to a single specific victim node by several minutes with different impact depending on the victim: if the victim is a merchant, it is susceptible to double spending attacks; if it is a miner, the attack wastes its computational power; finally, if it is a regular node, it is unable to contribute to the network by propagating the last version of the blockchain. The security of Bitcoin to network-based Attacks has been relatively less unexplored compared to other attack scenarios. Heilman et al. in [41] examines the eclipse attack on a single node in the context of Bitcoins p2p network Gervais et al. [36] consider other aspects of the centralization of Bitcoin and their consequences to the security of the protocol. In [13] authors presented an analysis of the vulnerabilities of the Bitcoin network from the networking viewpoint. Measuring and detecting routing attacks has seen extensive research on BGP hijack [13] [66] [77] and interception attacks [78].
Some countermeasures has been proposed to secure routing protocols that can prevent the above attacks [17] [37] [46] [58].

5 Critical Infrastructure

Critical Infrastructure represents an umbrella term used by governments to group all those resources that are essential for the economic, financial, and social system of a country. The Presidential Policy Directive 21 (PPD-21): Critical Infrastructure security and Resilience, issued by the President of United States in 2013, advances a national unity of effort to strengthen and maintain secure, functioning, and resilient Critical Infrastructure. PPD-21 identifies 16 Critical Infrastructure sectors: chemical, commercial facility, communication, critical manufacturing, dams, defence industrial base, emergency services, energy, financial service, food and agriculture, government facilities, health-care and public health, information technology, nuclear reactors, materials and waste, transportation system, and water and waste-water system, respectively [10]. The protection of these resources is crucial, because the destruction (or even the partial or momentary inability) could cause significant harm to the society, or worse, could jeopardize human lives. For example, in desert countries such as Qatar, Saudi Arabia, or the United Arab Emirates, attacking the Critical Infrastructures essential for the water supply (i.e., water refineries), would be tantamount to leaving the entire population without drinking water for the entire duration of the fault. The aforementioned Control Systems and protocols were put into operation decades ago, before the global spread of the Internet. At the time, security was not considered of paramount importance, as communication networks were closed and only very few people had access to information. The wide diffusion of the Internet of Things devices, occurred in the following years, made the security issues more sensitive. Indeed, the constant need for connectivity to networks and the interdependence between devices increase the need to make control systems and protocols more robust and resilient [22]. According to the Geneva Conventions of 1949, it is prohibited to attack, destroy, remove, or render useless objects indispensable to the survival of the civilian population, such as foodstuffs, agricultural areas for the production of foodstuffs, crops, livestock, drinking water installations and supplies, and irrigation works, for the specific purpose of denying them for their sustenance value to the civilian population or to the adverse party, whatever the motive, whether in order to starve out the civilians, to cause them to move away, or for any other motive [62]. Nevertheless, the increase of the attack surface due to the technologies has given way to numerous attacks on Critical Infrastructures, aimed at causing extensive damage to the victimized countries. In this section, we will take into account possible attacks related to three real-world scenarios: malware-guided attacks; attacks targeting the Supervisory Control And Data Acquisition (SCADA) systems; and attacks carried forward through the use of drones, respectively.

5.1 Scenario: Cyber Warfare targeting Critical Infrastructures

This scenario takes into account a Critical Infrastructure located within a country, which manages a critical resource. The Critical Infrastructure can be either a complex set of interconnected electrical components, as in the past, or a set of modern Internet of Things devices that communicate with each other. In both cases, the Critical Infrastructure exposes interfaces on the web, either to remotely receive commands or to show the status of the managed resource. The exposure to the web is necessary, to reduce the amount of dedicated personnel and to monitor the status of the critical resource in real time remotely. At the same time, however, the exposure to the web could lead to an increase of the attack surface, opening the doors to numerous attacks such as malware-base attacks and attacks on the SCADA systems, a subset of the Industrial Control Systems (ICSs)

Threat 1: Malware

The control systems and protocols that protect the Critical Infrastructure are usually a conglomerate of interconnected hardware and software resources. While hardware resources can be physically destroyed, malicious programs can be created to alter the behavior of the software resources. one historical example is

Stuxnet, a malicious worm that, back to 2010, is believed to be responsible for causing substantial damage to Iran's nuclear facilities. A more recent example is given by Triton, which exploited a critical switch placed in the wrong position to attack the industrial hardware in the Middle East. In general, old control systems did not take security into consideration because of their presence in restricted environments (i.e., due to the limited diffusion of the Internet). Once the control systems expose their interfaces to the current Internet, however, the danger is around the corner. Simple software errors or carefree third-party software execution can lead to external compromise, causing the temporary (or definitive) malfunction of the control software and jeopardizing the protected critical resource. Even worse, instead of provoking the destruction or the manumission of the control system, an attacker could take control of it from the outside, deceiving security systems and tampering with the critical resource without triggering security alarms.

Modern Critical Infrastructures are continually exposed to new threats due to the vulnerabilities and architectural weaknesses introduced by the extensive use of information and communication technologies (ICT). Of particular significance are the vulnerabilities in the communication protocols used in SCADA systems that are commonly employed to control industrial processes. In [34] authors investigated the impact of traditional ICT malware on SCADA systems, discussing the potentially damaging effects of computer malware created for SCADA systems. In [49] authors, after an introduction of industrial network protocol, design, and architecture, provided methods for risk and vulnerabilities assessment, implementing security and access controls, exception, anomaly, and threat detection that should help to prepare against the more and more sophisticated industrial network malware threats. In June 2017, ESET researchers discovered a malware considered the biggest threat to Critical Infrastructures since Stuxnet, named Industroyer. As its name suggests, Industroyer was designed to disrupt critical industrial processes being capable of doing significant harm to electric power systems. To make matters worse, the malware could also be refitted to target other types of Critical Infrastructures. The 2016 attack on Ukraine's power grid that deprived part of Kiev of power for an hour was caused precisely by a cyber attack. ESET researchers have suggested that the Win32/Industroyer malware would be capable of performing such an attack. Industroyer is a particularly dangerous threat, as it has the ability to control electricity substation switches and circuit breakers directly. According to ESET, it does this by using industrial communication protocols used worldwide in power supply infrastructure, transportation Control Systems, and other Critical Infrastructure systems (such as water and gas) [47].

Ukraine's power grid attack demonstrated that malicious actors seem to have extensive knowledge about Industrial Control Systems and Protocols. Terry Ray, the chief product strategist at Imperva, said "Since the industrial controls used in Ukraine are the same in other parts of Europe, the Middle East, and Asia, we could see more of these attacks in the future. And while these attackers seem to be content to disrupt the system, it is not outside the realm of possibility that they could take things a step further and inflict damage to the system themselves. Many of these industrial control systems have been in operation for years with little or no modification (no anti-virus updates or patches). This leaves them open to a wide range of cyber threats. It is therefore imperative that we find alternative measures to manage the risk. [47]. To mitigate the risk of ICS attacks, first, Critical Infrastructure administrators need to manage their system following the most simple and important best practices. Paul Edon, director at Tripwire, suggests that "security best practice includes selecting suitable frameworks such as NIST, ISO, CIS, ITIL to help direct, manage and drive security programs. It also means ensuring that the strategy includes all three pillars of security; People, Process, and Technology. Protection should apply at all levels; Perimeter, Network, and End Point. Finally, select the foundational controls that best suit your environment. There is a wealth of choice Firewalls, IDS/IPS, Encryption, Dual Factor Authentication, System Integrity Monitoring, Change Management, Off-line Backup, Vulnerability Management, and Configuration Management to name but a few." [47].

Threat 2: SCADA Systems Attacks

SCADA is a system of software and hardware elements that allows industrial organizations to: (i) control industrial processes locally or at remote locations; (ii) monitor, gather, and process real-time data; (iii) directly interact with devices such as sensors, valves, pumps, motors, and possibly others, through human-machine interface (HMI) software; and (iv) record events into a log file. SCADA systems are crucial for industrial organizations since they help to maintain efficiency, process data for smarter decisions, and communicate system issues to help mitigate downtime. The basic SCADA architecture begins with programmable logic controllers (PLCs) or remote terminal units (RTUs). PLCs and RTUs are microcomputers that communicate with an array of objects such as factory machines, HMIs, sensors, and end-devices, and then route the information from those objects to computers with SCADA software. The SCADA software processes distribute and display the data, helping operators and other employees analyzing the data and make important decisions based on them [12]. The exposure to the network provides the attackers with a wide range of possibilities. SCADA systems could be used to gather a lot of information, such as the facility's layout, critical safety thresholds to be taken into account, and much other critical information.

Academic research centers, after surveyed the most important cyber security problems on SCADA systems, are focusing on forward-looking security solutions. In [55] the authors analyzed several cyber-security incidents involving Critical Infrastructures and SCADA systems. They classified these incidents based on source sector, method of operations, impact, and target sector. Using this standardized taxonomy, they compared current and future SCADA incidents. In [56] the authors surveyed ongoing research and provide a coherent overview of the threats, risks, and mitigation strategies in the area of SCADA security. The research that has been done in this area provides long-term solutions and apply both industry and academic work to the problem. As such, these institutes remain very connected (by interacting regularly) with industry to make sure the research is gauged to provide a positive impact on the national infrastructure.

As already said for ICS in general, SCADA systems were often designed decades ago, when security was of little concern due to the closed nature of the communication networks. As these systems have been modernized, they have become interconnected and have started running more modern services such as web interfaces and interactive consoles (telnet/ssh), by implementing remote configuration protocols. Sadly, security has been left aside during the increased modernization of these systems. Indeed, these systems present very little implementations of standard security mechanisms such as encryption and authentication. The former is sometimes hard in these systems, due to the lack of processing power, the presence of slow links, and the presence of the legacy protocols. The primary issue with the slow links is the byte-time latency (i.e., time to transmit 1 byte) incurred from buffering the data for encryption. Although adding encryption to these systems is generally trivial, maintaining the other properties such as timing and data integrity with the encryption in place is not. Authentication is equally troublesome. Indeed, in the case of authentication, it is fairly common for the devices in the control space to use default passwords for access and control. Most of these default passwords are very easy to find when using search engines. This is a similar issue to network monitoring agents such as SNMP that often come configured by default with known public and private access phrases. The problem is further complicated by the move toward commercial, off-the-shelf (COTS) appliances and systems being integrated with the networks or part of the Control Systems themselves. While cutting costs and eliminating some of the proprietary nature of Control Systems, these appliances and systems bring with them the well-known passwords and vulnerabilities that each product may be subject to. Often these COTS systems may end up providing a point of entry for an attacker into the critical control network [75].

Threat 3: Drones

The advent of drones has introduced a whole new system of attacks aimed at mobile and non-mobile targets. In fact, in addition to the innocent fun related to making it fly to take breathtaking shots, there are some disturbing ways of use. A drone, in the hands of terrorists or malicious users, would make it easier to attack any target, causing massive damage. Strengthened by the fact that its limited size makes it extremely difficult to detect, the drone could be used for multiple purposes: a drone can be equipped with a camera to capture sensitive targets, such as alarm systems of a Critical Infrastructure, with the purpose of carrying out a first recognition useful for both checking security weaknesses and studying a detailed attack plan; a drone could also be equipped with weapons or small bombs, in order to be directly thrown at the target, causing explosions. It is not surprising that drones have been banned in several countries, such as Egypt, North Korea, and Iran, and restricted in others, such as Russia, the United Arab States, and Belgium. The paragraph will describe in detail the use of drones to attack Critical Infrastructures of a Country and analyze real cases, such as the attack of armed drones at the Russian military base in Syria, and Yemens Houthi drones attack an oil plant in southern Saudi Arabia.

Since their introduction on the retail market, the public opinion, as well as the research community, wondered about the actual danger of drones, opening the debate on what the threats and the benefits of this technology could be. In [69] [87] the author investigated about drones benefit, risks and legal consideration. In [59] authors, considering the significant number of non-military UAVs that can be purchased to operate in unregulated air space and the range of such devices, tested a specific UAV, the Parrot AR Drone version 2, and presented a forensic analysis of tests used to deactivate or render the device inoperative. They found that these devices are open to attack, which means they could be controlled by a third party. In the last few years, several episodes have helped to raise awareness among the institutions of the threat of UAVs against Critical Infrastructures. In December 2014, France revealed that unauthorized and unidentified UAS had breached the restricted airspace over 13 of the Countrys 19 nuclear plants during the preceding three months. These UAS were described as highly sophisticated civilian devices, and the flights over nuclear facilities appeared to be coordinated, with most of the violations occurring at night. In light of the increasing security concerns in Europe following terrorist attacks in France and Belgium, there is concern over the possible motives. There have been many notable incidents also in the United States. In early July 2016, the U.S. Department of Energy revealed that its Savannah River Site –which processes and stores nuclear materials– had experienced eight unauthorized flyovers in the span of two weeks. There have been unauthorized flyovers of a U.S. Navy nuclear submarine base, major sporting events, large public gatherings, and national monuments. UAS have crashed into the White House lawn and the New York Capitol, and there has been widespread documentation that they are being used to deliver contraband to prisons [20].

Most traditional radar cannot detect small, low-flying UAS, so this trend is particularly troubling. The majority of previous discussed documented flyovers were only discovered because of human detection –often by vigilant security personnel with keen eyesight. There have been efforts to improve upon the available technology, and a number of companies are marketing drone-detection security systems. However, even when they are detected, there are complications intercepting them and identifying the operators [20]. A possible solution is the design and implementation of anti-drones systems based on Jamming technologies. Recognizing and implementing security practices that meet states regulatory requirements are key to successfully managing potential security incidents associated with UAS. Although no single solution will fully mitigate this risk, there are several measures that can be taken to address UAS-related security challenges [64]: (i) research and implement legally approved counter-UAS technology; (ii) know the air domain around the facility and who has authority to take action to enhance security; (iii) update emergency/incident action plans to include UAS security and response strategies; (iv) build federal, state, and local partnerships for adaptation of best practices and information sharing; and (v) sensitize citizens and institutions to the problem, inviting anyone to report potential UAS threats to local law enforcement agency.

6 Conclusion

In this paper, we extended the classic pillars of Information Warfare to include the new threats posed by changes in our society as a result of technological advances in recent years. We described several real-case scenarios to show the possible impact that the new generation of Information Warfare could have in different aspects of modern society and economy. For each scenario, we identified one or more threats, investigating the state-of-the-art solutions for both the attack and defense methodologies existing in the literature. Finally, we identified open issues that still affect these fields, providing directions that could be useful to the development of more effective countermeasures.

Acknowledgement

This publication was partially supported by awards NPRP-S-11-0109-180242, UREP23-065-1-014, and NPRP X-063-1-014 from the QNRF-Qatar National Research Fund, a member of The Qatar Foundation. The information and views set out in this publication are those of the authors and do not necessarily reflect the official opinion of the QNRF.

References

1. The best bitcoin mining pools. https://www.bitcoinmining.com/bitcoin-mining-pools/ (Last checked April 2019)
2. The deep web is the 99% of the internet you can't google (Last checked April 2019), https://curiosity.com/topics/the-deep-web-is-the-99-of-the-internet-you-cant-google-curiosity/
3. Googles search knows about over 130 trillion pages (Last checked April 2019), https://searchengineland.com/googles-search-indexes-hits-130-trillion-pages-documents-263378
4. How to escape your political bubble for a clearer view (Last checked April 2019), https://www.nytimes.com/2017/03/03/arts/the-battle-over-your-political-bubble.html
5. Internet growth statistics (Last checked April 2019), https://www.internetworldstats.com/emarketing.htm

6. Breaking through censorship barriers, even when tor is blocked. https://blog.torproject.org/breaking-through-censorship-barriers-even-when-tor-blocked (Last checked July 2018)
7. Eu vs disinfo website. https://euvsdisinfo.eu/about/ (Last checked July 2018)
8. How trolls are ruining the internet. http://time.com/4457110/internet-trolls/ (Last checked July 2018)
9. A new study suggests fake news might have won donald trump the 2016 election. https://www.washingtonpost.com/news/the-fix/wp/2018/04/03/a-new-study-suggests-fake-news-might-have-won-donald-trump-the-2016-election/?noredirect=on\&utm_term=.d6e63f61fa06 ((Last checked July 2018))
10. Presidential policy directive – critical infrastructure security and resilience. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (Last checked July 2018)
11. Social media and censorship in china: how is it different to the west? http://www.bbc.co.uk/newsbeat/article/41398423/social-media-and-censorship-in-china-how-is-it-different-to-the-west (Last checked July 2018)
12. What is scada? https://inductiveautomation.com/what-is-scada (Last checked July 2018)
13. Apostolaki, M., Zohar, A., Vanbever, L.: Hijacking bitcoin: Routing attacks on cryptocurrencies. In: Security and Privacy (SP), 2017 IEEE Symposium on. pp. 375–392. IEEE (2017)
14. Bamman, D., O'Connor, B., Smith, N.: Censorship and deletion practices in chinese social media. First Monday **17**(3) (2012)
15. Bauer, K., McCoy, D., Grunwald, D., Kohno, T., Sicker, D.: Low-resource routing attacks against tor. In: Proceedings of the 2007 ACM workshop on Privacy in electronic society. pp. 11–20. ACM (2007)
16. Blockgeeks: What is cryptocurrency game theory: A basic introduction. https://blockgeeks.com/guides/cryptocurrency-game-theory/ (Last checked April 2019)
17. Boldyreva, A., Lychev, R.: Provable security of s-bgp and other path vector protocols: model, analysis and extensions. In: Proceedings of the 2012 ACM conference on Computer and communications security. pp. 541–552. ACM (2012)
18. Chabaud, F., Joux, A.: Differential collisions in sha-0. In: Annual International Cryptology Conference. pp. 56–71. Springer (1998)
19. Chu, Z., Gianvecchio, S., Wang, H., Jajodia, S.: Detecting automation of twitter accounts: Are you a human, bot, or cyborg? IEEE Transactions on Dependable and Secure Computing **9**(6), 811–824 (2012)
20. Dan Shea, A.E., Husch, B.: Drones and critical infrastructure. National Conference of States Legislatures (NCSL): http://www.ncsl.org/research/energy/drones-and-critical-infrastructure.aspx (December 2016), last checked April 2019
21. Dewey, J.: Democracy in education. The elementary school teacher **4**(4), 193–204 (1903)
22. Di Pietro, R., Oligeri, G.: Silence is golden: Exploiting jamming and radio silence to communicate. ACM Trans. Inf. Syst. Secur. **17**(3), 9:1–9:24 (Mar 2015). https://doi.org/10.1145/2699906, http://doi.acm.org/10.1145/2699906
23. Ding, F., Yang, Z., Chen, X., Guo, J.: Effective methods to avoid the internet censorship. In: 2011 Fourth International Symposium on Parallel Architectures, Algorithms and Programming. pp. 67–71. IEEE (2011)

24. Dingledine, R., Mathewson, N., Syverson, P.: Tor: The second-generation onion router. Tech. rep., Naval Research Lab Washington DC (2004)
25. Dobbertin, H.: Cryptanalysis of md4. In: International Workshop on Fast Software Encryption. pp. 53–69. Springer (1996)
26. Dobbertin, H.: Cryptanalysis of md5 compress. Tech. rep., Presented at the Rump Session of EuroCrypt (1996)
27. Dobbertin, H.: The status of md5 after a recent attack. Crypto-Bytes The technical newsletter of RSA Laboratories, a division of RSA Data Security, Inc. **2**(2) (1996)
28. Dobbertin, H.: Ripemd with two-round compress function is not collision-free. Journal of Cryptology **10**(1), 51–69 (1997)
29. Elyashar, A., Bendahan, J., Puzis, R.: Has the online discussion been manipulated? quantifying online discussion authenticity within online social media. arXiv preprint arXiv:1708.02763 (2017)
30. Eperiesi-Beck, E.: The threat quantum computers pose to modern security. `https://www.scmagazineuk.com/the-threat-quantum-computers-pose-to-modern-security/article/709472/` (Last checked April 2019)
31. Ferrara, E.: Disinformation and social bot operations in the run up to the 2017 french presidential election (2017)
32. Fokin, A., et al.: Internet trolling as a tool of hybrid warfare: The case of latvia. Tech. rep., NATO Strategic Communications Centre of Excellence (1996)
33. Forelle, M., Howard, P., Monroy-Hernández, A., Savage, S.: Political bots and the manipulation of public opinion in venezuela. arXiv preprint arXiv:1507.07109 (2015)
34. Fovino, I.N., Carcano, A., Masera, M., Trombetta, A.: An experimental investigation of malware attacks on scada systems. International Journal of Critical Infrastructure Protection **2**(4), 139–145 (2009)
35. Gertz, N.: Censorship, Propaganda, and the Production of 'Shell Shock' in World War I. Disciplinary Press, Oxford, UK (2009)
36. Gervais, A., Karame, G., Capkun, S., Capkun, V.: Is bitcoin a decentralized currency? IEEE security & privacy **12**(3), 54–60 (2014)
37. Gill, P., Schapira, M., Goldberg, S.: Let the market drive deployment: A strategy for transitioning to bgp security. In: ACM SIGCOMM Computer Communication Review. vol. 41, pp. 14–25. ACM (2011)
38. Guriev, S.M., Treisman, D.: How modern dictators survive: Cooptation, censorship, propaganda, and repression. CEPR Discussion Paper No. DP10454 (2015)
39. Handschuh, H., Knudsen, L.R., Robshaw, M.J.: Analysis of sha-1 in encryption mode. In: Cryptographers Track at the RSA Conference. pp. 70–83. Springer (2001)
40. Hegelich, S., Janetzko, D.: Are social bots on twitter political actors? empirical evidence from a ukrainian social botnet. In: Tenth International AAAI Conference on Web and Social Media (2016)
41. Heilman, E., Kendler, A., Zohar, A., Goldberg, S.: Eclipse attacks on bitcoin's peer-to-peer network. In: USENIX Security Symposium. pp. 129–144 (2015)
42. Heins, M.: The brave new world of social media censorship. Harv. L. Rev. F. **127**, 325 (2013)
43. Hilvert, J.: Blue pencil warriors: Censorship and propaganda in World War II. University of Queensland Press (1984)
44. Hintz, A.: Social media censorship, privatized regulation, and new restrictions to protest and dissent. Rowman & Littlefield (2015)
45. Howard, P.N., Kollanyi, B.: Bots, #strongerin, and #brexit: computational propaganda during the uk-eu referendum. Available at SSRN 2798311 (2016)

46. Hu, Y.C., Perrig, A., Sirbu, M.: Spv: Secure path vector routing for securing bgp. ACM SIGCOMM Computer Communication Review **34**(4), 179–192 (2004)
47. Ismail, N.: New malware represents biggest threat to critical infrastructure. `https://www.information-age.com/new-malware-represents-biggest-threat-critical-infrastructure-123466733/` (June 2017 Last checked July 2018)
48. Keshen, J.: Propaganda and censorship during Canada's Great War. University of Alberta (1996)
49. Knapp, E.D., Langill, J.T.: Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems. Syngress (2014)
50. Kumar, S., Cheng, J., Leskovec, J., Subrahmanian, V.: An army of me: Sockpuppets in online discussion communities. In: Proceedings of the 26th International Conference on World Wide Web. pp. 857–866. International World Wide Web Conferences Steering Committee (2017)
51. La Morgia, M., Mei, A., Raponi, S., Stefa, J.: Time-zone geolocation of crowds in the dark web. In: 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS). pp. 445–455. IEEE (2018)
52. MacArthur, J.R.: Second front: Censorship and propaganda in the 1991 Gulf War. Univ of California Press (2004)
53. Mason, A.: CCSP Self-Study: Cisco Secure Virtual Private Networks (CSVPN). Pearson Higher Education (2004)
54. Mihaylov, T., Georgiev, G., Nakov, P.: Finding opinion manipulation trolls in news community forums. In: Proceedings of the nineteenth conference on computational natural language learning. pp. 310–314 (2015)
55. Miller, B., Rowe, D.C.: A survey scada of and critical infrastructure incidents. RIIT **12**, 51–56 (2012)
56. Nicholson, A., Webber, S., Dyer, S., Patel, T., Janicke, H.: Scada security in the light of cyber-warfare. Computers & Security **31**(4), 418–436 (2012)
57. Nobori, D., Shinjo, Y.: {VPN} gate: A volunteer-organized public {VPN} relay system with blocking resistance for bypassing government censorship firewalls. In: Proceedings of the 11th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 14). pp. 229–241 (2014)
58. van Oorschot, P.C., Wan, T., Kranakis, E.: On interdomain routing security and pretty secure bgp (psbgp). ACM Transactions on Information and System Security (TISSEC) **10**(3), 11 (2007)
59. Peacock, M., Johnstone, M.N.: Towards detection and control of civilian unmanned aerial vehicles. SRI Security Research Institute, Edith Cowan University, Perth, Western (2013)
60. Preneel, B., Govaerts, R., Vandewalle, J.: Differential cryptanalysis of hash functions based on block ciphers. In: Proceedings of the 1st ACM Conference on Computer and Communications Security. pp. 183–188. ACM (1993)
61. Ratkiewicz, J., Conover, M.D., Meiss, M., Gonçalves, B., Flammini, A., Menczer, F.M.: Detecting and tracking political abuse in social media. In: Fifth international AAAI conference on weblogs and social media (2011)
62. Roberts, A.: Documents on the Laws of War. HeinOnline (2000)
63. Saarinen, M.J.O.: Cryptanalysis of block ciphers based on sha-1 and md5. In: International Workshop on Fast Software Encryption. pp. 36–44. Springer (2003)
64. Security, U.H.: Unmanned aircraft systems (uas) - critical infrastructure. `https://www.dhs.gov/uas-ci` (Last checked July 2018)
65. Shadmehr, M., Bernhardt, D.: State censorship. American Economic Journal: Microeconomics **7**(2), 280–307 (2015)

66. Shi, X., Xiang, Y., Wang, Z., Yin, X., Wu, J.: Detecting prefix hijackings in the internet with argus. In: Proceedings of the 2012 Internet Measurement Conference. pp. 15–28. ACM (2012)
67. Shmatikov, V., Wang, M.H.: Timing analysis in low-latency mix networks: Attacks and defenses. In: European Symposium on Research in Computer Security. pp. 18–33. Springer (2006)
68. Shor, P.W.: Algorithms for quantum computation: Discrete logarithms and factoring. In: Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on. pp. 124–134. Ieee (1994)
69. Smith, K.W.: Drone technology: Benefits, risks, and legal considerations. Seattle J. Envtl. L. **5**, i (2015)
70. Starbird, K.: Examining the alternative media ecosystem through the production of alternative narratives of mass shooting events on twitter. In: Eleventh International AAAI Conference on Web and Social Media (2017)
71. Sun, Y., Edmundson, A., Vanbever, L., Li, O., Rexford, J., Chiang, M., Mittal, P.: {RAPTOR}: Routing attacks on privacy in tor. In: 24th {USENIX} Security Symposium ({USENIX} Security 15). pp. 271–286 (2015)
72. Waldorf, L.: Censorship and propaganda in post-genocide Rwanda. Pluto Press, London (2007)
73. Wang, Y., Ji, P., Ye, B., Wang, P., Luo, R., Yang, H.: Gohop: Personal vpn to defend from censorship. In: 16th International Conference on Advanced Communication Technology. pp. 27–33. IEEE (2014)
74. Winter, P., Lindskog, S.: How the great firewall of china is blocking tor. USENIX-The Advanced Computing Systems Association (2012)
75. Yardley, T.: Scada: issues, vulnerabilities and future directions. ; login:: the magazine of USENIX & SAGE **33**(6), 14–20 (2008)
76. Zannettou, S., Caulfield, T., De Cristofaro, E., Sirivianos, M., Stringhini, G., Blackburn, J.: Disinformation warfare: Understanding state-sponsored trolls on twitter and their influence on the web. arXiv preprint arXiv:1801.09288 (2018)
77. Zhang, Z., Zhang, Y., Hu, Y.C., Mao, Z.M.: Practical defenses against bgp prefix hijacking. In: Proceedings of the 2007 ACM CoNEXT conference. p. 3. ACM (2007)
78. Zhang, Z., Zhang, Y., Hu, Y.C., Mao, Z.M., Bush, R.: ispy: Detecting ip prefix hijacking on my own. IEEE/ACM Transactions on Networking (TON) **18**(6), 1815–1828 (2010)