Source: © Kacper Pempel, Reuters.

Global Power Shifts

Cyber Capabilities as a New Resource of Power

Conflicts in the Digital Sphere

Jason Chumtong / Christina Stolte

Cyber capabilities are becoming increasingly important in international relations. States with the ability to conduct cyber operations are in a strong position to expand their scope of influence in the international arena. This is particularly true for small and medium-sized countries with few traditional power resources, as cyber capabilities allow them to seriously weaken more powerful states.

Invisible Shifts of Power

Over the last 20 years, the growth of China and other emerging nations has given rise to a tectonic shift in the global power structure.[1] Despite today's global players having been on the fringes and largely excluded from the processes of international decision-making at the turn of the millennium, today it is hard to imagine decisions of global significance being made without the involvement of countries like China and India. The rapid rise of these former emerging nations is particularly evident in the economic and military spheres. Their increased power is impressively demonstrated in their global rankings on GDP, economic growth, military spending, and technology. Glittering skyscrapers, nuclear technology, and spectacular space missions all herald this new power, exploiting most of the usual power symbols of the late 20th century in their quest to flaunt their newly acquired capabilities and status.

In parallel, a power shift of a less visible kind has almost gone unnoticed by the international community because it is silent, invisible, and shows no conspicuous demonstrations of power: the power shift in cyberspace.[2] Over the last decade, a number of countries have increasingly focused on developing and expanding their cyber capabilities. They have thus found new ways of gaining power by influencing international decisions and events to their own advantage.

Similar to the rise of the Global South, we are experiencing a very surprising and comparatively rapid power shift that has occurred within just a few years. This is partly because cyberspace – defined as a virtual space that encompasses the global network of all information technology infrastructures – is, on the whole, a new sphere of state action. This sense of surprise is also due to the unusual nature of this means of exercising power. Unlike the traditional resources that nations draw on in order to compete for power and influence, such as their military capabilities, economic strength, and prosperity, cyber power is difficult to quantify and rarely truly visible. But even though it is an invisible, largely intangible form of power, it still complies with the traditional definition of power as the ability to enforce a nation's interests[3] vis-à-vis another country, as contended in the National Cyber Power Index.[4] In this way, cyber espionage and cyberattacks may inflict severe financial and even humanitarian damage on other countries. Yet, even simple influence campaigns could endanger the credibility or even stability of another country and severely weaken the opponent by spreading propaganda and targeted disinformation.[5]

The analogue world has also always had an "invisible" sphere for pursuing strategic objectives, namely the intelligence services. Small and middle powers compensate for their lesser military strength by pursuing a wide range of intelligence activities. The battle between states to gain power through digital means can, therefore, be seen as an extension of this sphere because it has a low threshold for entry. Although terms such as "cyber powers" recall the world's leading, most technologically advanced countries, the new cyber powers are not only found among the usual global players.

Instead, they include nations with few conventional capabilities for exercising power on the international stage.

Digital technology affords new opportunities to smaller states that lack traditional capabilities in this respect to influence international relations.

However, great powers such as the US and China continue to be the dominant players when exercising cyber power.[6] But while cyberspace is merely another sphere for the established great powers to assert their interests and exercise power, digital technology affords new opportunities to smaller states that lack traditional capabilities in this respect to influence international relations, and aggressively pursue their interests. In addition to this power shift towards cyberspace, whose importance has grown significantly compared to that of the traditional military sphere, another shift has occurred in favour of countries that recognised and exploited the potential of cyber capabilities at an early stage.

This report turns the spotlight on Russia, Venezuela, and Iran as emerging cyber powers. It uses the case studies of countries with varying degrees of influence to highlight the broad spectrum and diversity of this new form of power and to raise awareness of the opportunities presented by this new capability – not only for the most technologically advanced cyber powers, but also for second- and third-tier countries in international relations.

The Internet as an Arena for International Power Struggles

To understand the role of cyberspace as an arena for international power struggles and conflicts, it helps to look at different stages of international conflicts in the analogue world. Let us imagine that country A expels the ambassador of country B. Instead of responding by summoning the ambassador, country B decides to send its tanks to its border. If country A then also responds with "tougher" measures, such as firing warning shots at the tanks, the confrontation escalates from a diplomatic to a military level. Every action taken in this game of tit for tat ramps up the aggression. In conflict theory, these stages are mapped on escalation scales or escalation ladders.[7] They aim to show which mode of attack corresponds to which level of escalation. The variability of cyberattacks can also be represented on a scale, as shown below.

The Cyber Escalation Ladder:[8]

Level 1 Preparation: recruiting and training hackers; preparing attacks

Level 2 Minor harassment: influencing the information space through propaganda and fake news; cyber espionage and data theft via trojans

Level 3 Major harassment: temporary shutdown of services via DDoS attacks (Distributed Denial of Service); Swatting (hoax calls to emergency services, police, fire services, emergency doctors)

Level 4 Minor damaging attacks: destruction of critical data; targeted assaults on military infrastructure via malware (e.g. Stuxnet)[9]

Level 5 Major damaging attacks: targeted impairment of military capabilities, destruction of military infrastructure (no examples to date)

Level 6 Catastrophic attacks: permanent damage to the civilian population due to destruction of civilian infrastructure (no examples to date)

Level 7 Existential attacks: damage on the scale of a nuclear pre-emptive strike (no examples to date)

Intuitively, cyberspace offers a great range of possibilities for conflicts to escalate, especially because every connection to the Internet is, due to digital networking, a potential weak point and provides attack vectors. Yet, as effective means for counterattacks the cyberspace has few advantages. These are the reasons:

1. Cyberattacks are not target agnostic. While conventional weapons can be used against a variety of different targets without major adjustments, cyberattacks have to be adapted to their particular target. In principle, no matter whether a missile is fired at a building or a vehicle, it is likely to cause damage when it detonates.[10] However, a trojan that has been designed for system X usually does not work in system Y.

2. Cyberattacks are inflexible. The large volume of different (operating) systems used in information and telecommunication technology makes selecting an attack vector and preparing a suitable attack very time consuming. Chris Inglis, former Deputy Director of the NSA, confirms that a cyberattack is 90 per cent preparation, making it unsuitable for rapid counterreactions.[11]

3. Cyberattacks are short-lived. Since software, as a non-physical component of a technology, can be developed with relatively few resources, cyberspace is subject to dynamic change. Successful cyberattacks act as a catalyst for this development, since as a reaction the respective weak points within the software are fixed in the long term. The myth of the cyber offence purports that the attacker always has an advantage over the defender. This is countered by Paul Nakasone, Director of the NSA, who says that offensive cyber capabilities rarely last more than six months.[12]

With this in mind, the benefit of cyberattacks clearly lies above all in their ability to manipulate an enemy's use of cyberspace, and to covertly infiltrate its information networks.[13] Essentially, they are conventional methods of espionage and manipulation. They have fewer advantages for conventional attacks but are generally used to support modern military operations.[14] Contrary to Clausewitz's dichotomy of war and peace, cyberattacks operate in a space between the two that remains a grey area in international law.[15] However, low-threshold cyber operations provide aggressor states with a way to increase their influence precisely due to the absence of an open declaration of war, and the low risk of escalation. This is a decisive factor, especially vis-à-vis countries with greater military might.

In cyberspace, the weak spot is often people and their careless internet use, as opposed to systems.

Cyber Superpowers and Rising Cyber Powers: The Spectrum of Cyber Capabilities

The success of a cyberattack does not necessarily come down to the complexity of the malware, the quality of the resources available, or the skill of the hackers. The key to effective espionage is infiltrating systems via the simplest methods of obtaining passwords and, hence, accessing more gateways. Gateways such as phishing emails or infected USB sticks are frequently used and illustrate how easy it is for malware to get into the system. In cyberspace, the weak spot is often people, as opposed to systems. Careless internet use, using default passwords on network routers, reusing private passwords for professional applications, or even storing access data in text files or emails – these are just a few of the critical vulnerabilities that open the door to cyberattacks. The following examples from Russia, Iran, and Venezuela reveal the extent to which cyberattacks are currently being used to manipulate the global balance of power.

Influencing public opinion: With disinformation campaigns tailored towards specific national contexts, Russia actively contributes to the polarisation of societies in Western democracies. Source: © Gleb Garanich, Reuters.

Russia

As a traditional great power and former superpower in the duel with the US, it is hardly surprising that Russia is active in cyberspace. Over the last decade, Russia has invested enormously in regaining its former status and implemented an extensive rearmament programme. Digital technologies and cyber capabilities have played a central role from the start. As early as 2013, Russia's Chief of the General Staff Valery Gerasimov laid the groundwork for Russia's new approach to power projection. This involved the adoption of disinformation and other non-military measures and far exceeded the concepts underpinning conventional warfare. Various aspects of cyber warfare, such as cyberattacks on other nations' institutions and infrastructure and online influence campaigns to manipulate political opinion formation, were combined in a holistic approach. This soon bridged the gap between conventional and cyber warfare that had long prevailed in the West, and Russia quickly recognised and harnessed the potential of this new way of exerting its influence.[16]

Russia's information warfare aims at fomenting social discord and political chaos.

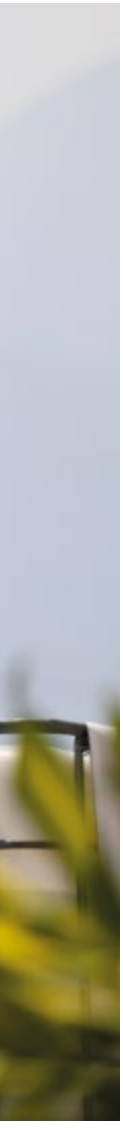
Russia adopted a pioneering role in cyberspace from the outset. For example, the first known cyberattack – targeting government bodies in Estonia's capital Tallinn in 2007 – is attributed to Russia. Russia was also responsible for the

first cyberattack on critical energy infrastructure when hackers disrupted electricity supplies in the Ukrainian region of Ivano-Frankivsk in 2015. Cyberattacks on the German Bundestag in 2015 and on US government institutions between 2014 and 2016, orchestrated by Russian intelligence services and carried out by hacker groups such as APT28, also known as Fancy Bear, grabbed headlines in Germany for the first time as they illustrated how even seemingly secure government institutions, such as the White House, were vulnerable to attacks. Today, Russia can look back on 15 years of international cyber activities and is one of the so-called cyber superpowers, along with the United States, the United Kingdom, Israel, and China.[17]

In addition to the cyberattacks described above, which Russia has perfected over the past 15 years, the former superpower is also making its mark around the world in another area of cyber warfare. Global disinformation campaigns as well

Contrasts: Despite not even being able to provide its people with basic services, the Venezuelan government is a serious player in the field of disinformation. Source: © Manaure Quintero, Reuters.

as those tailored towards specific national contexts, have cast doubt on the credibility of hostile governments, vilified political opponents, and actively contributed to the polarisation of Western democracies.[18] Interestingly, these campaigns are not primarily about Russia, nor does the content directly or indirectly pertain to Russia. Rather, this form of information warfare aims at fomenting social discord and political chaos, thus systematically weakening hostile nations from within. The means used to achieve this are as simple as they are effective. With the help of a few hundred employees, fake social media accounts, troll armies, and bots, the Internet Research Agency in St Petersburg has succeeded in stirring up controversy, inciting social protests, and intervening in electoral processes.[19] Exercising this kind of influence is technically simple but has far-reaching effects. This was recently demonstrated not least in the 2016 US presidential election campaign, which Russia manipulated with hacker attacks and social media campaigns in favour of Donald Trump as detailed in the report by Special Counsel Robert Mueller.[20] There have been many proven cases of Russian interference, including the independence referendum in Catalonia (2017), the Brexit referendum (2016), and the international coverage on Russian opposition leader Alexei Nawalny. These all complete the picture of an almost omnipresent cyber power that subversively intervenes in the political discourses and electoral processes of other nations.



Venezuela

By contrast, Venezuela is a more surprising player in the realm of cyberspace. This South American country has been in the throes of a humanitarian crisis for many years. Its people are plagued by food shortages, hyperinflation, and abject poverty, with one-fifth of Venezuela's population having fled from their desperate circumstances since 2018. But despite the country neither being able to feed its people nor provide reliable supplies of electricity and water, it is a serious player in the field of digital subversion. It is with good reason that, in 2019, Oxford University's Global Inventory of Organised Social Media Manipulation ranked the South American nation as one of the world's leading manipulators in terms of cyber troop capacity.[21]

The Venezuelan troll army tries to control the narrative of the regime by disseminating fake news on a massive scale.

What may come as a surprise for many is that Venezuela has been pursuing a cyber strategy for several years – a strategy that international analysts describe as extremely powerful, especially as regards disseminating propaganda. Even back in 2010, President Hugo Chávez pursued a strategy of actively using social media to spread his political message and mobilise support. By 2017 at the latest, Venezuela was building its cyber troops to arm itself for information warfare in cyberspace according to a leaked document from the Venezuelan Interior Ministry titled "Project to Create a Troll Army of the Bolivarian Revolution".[22]

According to experts, the Venezuelan troll army is at least 500 persons strong. Reinforced by digital bots, they besiege social networks such as YouTube, Facebook, Instagram, Telegram, WhatsApp, and especially Twitter, seeking to ensure Venezuela's regime controls the narrative by spreading its political messages, disrupting the democratic opposition's social media communications, and disseminating fake news on a massive scale.[23] The Venezuelan cyber army's "disinformation units" have a military-style structure, with each unit operating over one thousand social media accounts. At the height of the information war, such as during protests against Hugo Chávez's successor, Nicolás Maduro, or the US decision to impose international sanctions on Venezuela in 2019, research shows that more than 80 per cent of pro-regime social media traffic was generated by automated bots. However, unlike other states that manipulate social networks for propaganda purposes, Venezuela has relatively large numbers of flesh-and-blood trolls at work.[24] They are partly

paid in food vouchers, which, in this crisis-ridden country, are more valuable than cash in view of the prevailing food shortages and hyperinflationary national currency.

Venezuela's cyber activities also go beyond its national borders. According to the Atlantic Council, Venezuela is the first country in Latin America to use cybertechnology to spread strategic propaganda – and not only within its own territory.[25] Indeed, a comparative study by Oxford University shows that the economically impoverished country is in fact among the world's leaders in terms of its capacity for running information campaigns with a global reach.[26] The last few years have borne witness to Venezuela's success in using this capability to exert influence in other countries. For example, Venezuela has interfered in a variety of socio-political controversies, not only in Latin America but also in Spain, thanks to the use of fake social media accounts and automated dissemination tools, sometimes in conjunction with Russia. There is evidence that it has fuelled social tensions and helped to radicalise emerging protest movements.[27] It is no coincidence that precisely those states that had previously spoken out against the Maduro regime have found themselves the target of Venezuela's subversive disinformation campaigns.[28] The various protests that spread like wildfire in Chile, Ecuador, and Colombia and spilled over into the entire region in autumn 2019 cannot solely be attributed to Venezuela's actions; however, the country's successful interference campaigns impressively demonstrate the potential of digital technologies to project power in countries that lack traditional resources for doing so, such as Venezuela.

Iran

The Islamic Republic of Iran began developing its cyber capabilities at an early stage. Against the backdrop of the painful experience of the 2009 Green Revolution social media campaigns, which placed the regime under immense pressure, and the devastating cyberattack on Iranian nuclear enrichment facilities caused by the Stuxnet computer worm in 2010, Iran's revolutionary leader, Ali Khamenei, set up the Supreme Council of Cyberspace in early 2012. The Council is responsible for all decisions relating to cyber policy. It censors any web content that it deems inappropriate, counters the (relatively frequent) cyberattacks on Iran, and is actively building the country's capacity to carry out cyberattacks on its opponents. With its lack of conventional military capabilities and economic isolation due to strict international sanctions, Iran sees the development and use of cyber technology as a way of acquiring asymmetric warfare capabilities, thus enhancing its ability to project power.

Iran has evolved from an early cyber victim to an offensive cyber power.

While Iran still lags behind Russia, the US, and Israel in terms of cyber capabilities, the Islamic Republic has made great strides in recent years, evolving from an early cyber victim to an offensive cyber power capable of inflicting serious damage, even on countries with superior technology.[29] Intentionally, its attacks are not directed against government or military institutions, but instead target private-sector businesses in countries it deems hostile. For example, in 2012 Iran inflicted enormous financial damage through DDoS attacks on more than a dozen major US banks, forcing individual banks to invest tens of millions of dollars in protecting themselves against future Iranian hacking. On Wall Street, too, a hacker group close to Iran was able to cause considerable damage in 2013 – at least temporarily – by hacking the Twitter account of the Associated Press news agency. As a result, it spread fake news about explosions at the White House and alleged injuries to the US president. By the time this news was identified as fake, the Dow Jones had fallen 150 points and wiped out 136 billion US dollars in value.[30]

In addition to technically simple hacker attacks with a serious financial impact on their victims,

Iran's cyber capabilities also include disinformation campaigns. Particularly in the Arab world, Iran is fighting for influence via social media and using concerted propaganda campaigns to weaken its rival, Saudi Arabia. In addition to normal computer-based social media campaigns, Iran has created elaborate imitations of Arab news sites to disseminate the Iranian narrative as well as to publish content that is critical of the Saudi government throughout the Arab region.[31]

As an international pariah state with very few conventional resources for wielding influence, in less than a decade Iran has evolved into a serious player in the field of cyber warfare. It may not have joined the ranks of the cyber superpowers, but it is skilfully pursuing its regional power ambitions in cyberspace.

Conclusion

As different as the above examples of cyber powers large and small are, they all highlight a clear trend: Cyber capabilities are becoming more important in international relations. Countries capable of conducting cyber operations are witnessing a noticeable increase in their power, while countries without this capability are experiencing a loss of influence on the international stage.

Interestingly, traditional sources of power, such as military and economic strength, are not a prerequisite for success in cyberspace. It is true that the premier league of cyber powers also includes many traditional major powers in its ranks. But states need very few resources to build their cyber capabilities and exploit them to project influence, as the examples of international outsiders like Iran and Venezuela demonstrate. In some ways, cyber capabilities even seem ideally suited to allowing small and medium-sized countries to increase their influence because they represent an effective tool of asymmetric warfare. Even though they require relatively few resources and low-threshold technology, they have the potential to inflict considerable damage when deployed against other countries. Attacks on poorly protected public authorities, businesses, or even infrastructure can cause serious damage to other countries.

In the field of information warfare, states that were never previously on the radar as global players are now increasing their international influence.

The risks for the attacker are reasonably low because attribution of the attacks is usually difficult and time-consuming. On top of this, the evidence is seldom clear, and consistent denial of any involvement is part and parcel of cyber warfare.[32] This is also one of the key differences from previous power struggles at the international level. While the global battle for power and influence has always been accompanied by visible demonstrations of power and the accumulation of status symbols, the struggle in cyberspace takes place under the radar.

This makes it especially difficult to identify shifts of power occurring today. Particularly in the field of information warfare, an area of growing importance in both national and international conflicts, states that were never previously on the radar as global players are now increasing their international influence. Yet, these countries recognised the potential of digital technologies at an early stage and are exploiting them with great success. Many of them have a wealth of experience in this respect due to having deployed the tools of information warfare against their own citizens and political opponents for many years. They can now direct this expertise towards other countries to wield global influence.

Government bodies in Germany are strongly aware of the danger, as documented by the sections on cyber activities in the country's annual domestic intelligence reports and the creation of the National Cyberdefence Centre already in

2011. Yet, the public is still largely unaware of the scale of the subversive cyber activities carried out by foreign governments. They are not only designed to spy on public authorities and businesses, but also use disinformation campaigns to manipulate public opinion – and hence the population. There is a need for widespread awareness campaigns to highlight specific attempts by foreign states to exert their influence. These should be conducted in such a way that they attract media attention and actively raise public awareness of this subtle form of external meddling. Germany needs to raise public awareness of the scale and potential threat posed by cyberattacks if it is to avoid becoming their target.

– translated from German –

Jason Chumtong is Desk Officer for Artificial Intelligence at the Konrad-Adenauer-Stiftung.

Dr. Christina Stolte is Desk Officer for the Andean States, Rule of Law Programme Latin America, and the Regional Programme Political Participation of Indigenous People at the Konrad-Adenauer-Stiftung.

1 Dargin, Justin 2013: The Rise of the Global South, Philosophical, Geopolitical and Economic Trends of the 21st Century, Singapore.
2 Kello, Lucas 2017: The Virtual Weapon and International Order, New Haven.
3 Here, power is defined according to Max Weber as "the chance that an individual in a social relation can achieve his or her own will even against the resistance of others". Weber, Max 1972: Wirtschaft und Gesellschaft: Grundriß der verstehenden Soziologie, 5th edition, Tübingen, p. 28. Conventional resources in the global pursuit of power include a country's military capabilities (size of its army and arsenal, technical and logistical capacities) and its economic power (GDP; prosperity and degree of economic development).
4 Rosenbach, Eric 2020: A Note to Readers, in: Voo, Julia / Hemani, Irfan / Jones, Simon / DeSombre, Winnona / Cassidy, Dan / Schwarzenbach, Anina (eds.): National Cyber Power Index 2020. Methodology and Analytical Considerations, Belfer Center for Science and International Affairs, Sep 2020, p.iv, in: https://bit.ly/37MeWLO [25 Feb 2021].
5 Prier, Jarred 2017. Commanding the Trend: Social Media as Information Warfare, in: Strategic Studies Quarterly 11: 4, pp. 50–85, in: https://bit.ly/3r3N2Tf [2 Mar 2021]; Harknett, Richard J. / Smeets, Max 2020: Cyber campaigns and strategic outcomes, Journal of Strategic Studies, 4 Mar 2020, in: https://bit.ly/3bSnoum [2 Mar 2021].
6 Voo et al. 2020, n. 4.
7 Kahn, Herman 2010: On Escalation. Metaphors and Scenarios, London.
8 Kostyuk, Nadiya / Powell, Scott / Skach, Matt 2018: Determinants of the Cyber Escalation Ladder, in: The Cyber Defense Review 3: 1, pp. 123–134, in: https://bit.ly/3sGDY77 [2 Mar 2021].
9 Baezner, Marie / Robin Patrice 2017: Hotspot Analysis: Stuxnet, Center for Security Studies (CSS), Oct 2017, in: https://bit.ly/3aShhqz [13 Jan 2021].
10 Borghard, Erica D. / Lonergan Shawn W. 2019: Cyber Operations as Imperfect Tools of Escalation, in: Strategic Studies Quarterly, 13: 3, pp. 128 ff., in: https://jstor.org/stable/26760131 [2 Mar 2021].
11 Inglis Chris 2018: Illuminating a New Domain: The Role and Nature of Military Intelligence, Surveillance, and Reconnaissance in Cyberspace, in: Lin, Herbert / Zegart, Amy (eds.): Bytes, Bombs, and Spies. The Strategic Dimensions of Offensive Cyber Operations, Washington, pp. 19–44, here: p. 25.
12 Eliason, William T. 2019: An Interview with Paul M. Nakasone, in: Joint Force Quarterly 92, pp. 7 f., in: https://bit.ly/3qXAhcI [13 Jan 2021].
13 Wiggen, Johannes 2020: Im Zustand des Unfriedens. Staatliche Cyberoperationen unterhalb der Schwelle bewaffneter Konflikte, Die Politische Meinung 565, Konrad-Adenauer-Stiftung, pp. 24–29, in: https://bit.ly/3b5tqsq [2 Mar 2021].
14 Schulze, Matthias 2021: 23 WTF ist Cyber Eskalation? Eskaliert der Hackback?, Perception, Podcast, 1 Jan 2021, in: https://bit.ly/2ZOy47D [25 Feb 2021].

15 International Committee of the Red Cross 2010: Cyber warfare, 29 Oct 2010, in: https://bit.ly/3r9TLv5 [2 Mar 2021].
16 Akimenko, Valeriy / Giles, Keir 2020: Russia's Cyber and Information Warfare, Asia Policy 15: 2, pp. 67–75, 29 Apr 2020, in: https://bit.ly/3kAq0B7 [2 Mar 2021].
17 Voo, Julia / Hemani, Irfan / Jones, Simon / DeSombre, Winnona / Cassidy, Dan / Schwarzenbach, Anina 2020: Reconceptualizing Cyber Power. Cyber Power Index Primer, Report der China Cyber Policy Initiative, Apr 2020, in: https://bit.ly/302wwap [25 Feb 2021].
18 Buchanan, Ben 2020: The Hacker and the State. Cyber Attacks and the New Normal of Geopolitics, Cambridge.
19 Chen, Adrian 2015: The Agency, The New York Times Magazine, 2 Jun 2015, in: https://nyti.ms/3bDJQan [25 Feb 2021]; Kosoff, Maya 2017: How Russia Secretly Orchestrated Dozens of U.S. Protests, Vanity Fair, 30 Oct 2017, in: https://bit.ly/3dLVwe4 [25 Feb 2021].
20 Mueller, Robert S. 2019: Report on the Investigation into Russian Interference in the 2016 Presidential Election, U.S. Department of Justice, Mar 2019, in: https://bit.ly/3dLCvIs [25 Feb 2021].
21 Bradshaw, Samantha / Howard, Philip N. 2019: The Global Disinformation Order. 2019 Global Inventory of Organised Social Media Manipulation, Working Paper 2, Project on Computational Propaganda, in: https://bit.ly/37Na9tz [25 Feb 2021].
22 Ministerio de Interior, Justicia y Paz 2017: Proyecto de Formación del Ejército de Trolls de la Revolución Bolivariana, in: https://bloom.bg/3pQAcpX [25 Feb 2021].
23 Transparencia Venezuela 2019: La desinformación, estrategia intencional del Poder, Informe de Corrupción, in: https://bit.ly/3bHp5KS [25 Feb 2021].
24 Bradshaw, Samantha / Howard, Philip N. 2019, Case Studies – Collated, Nov 2019, Venezuela, pp. 126–128, in: https://bit.ly/3knD7VV [2 Mar 2021].
25 Suárez Pérez, Daniel / Ponce de Leon Rosas, Esteban 2021: Digital Autocrazy. Maduro's control of the Venezuelan information environment, Atlantic Council, Mar 2021, in: https://bit.ly/3uP6DYR [14 Apr 2021].
26 Bradshaw / Howard 2019, n. 21.
27 Coscojuela, Saraí / Quintero, Luisa 2019: Tropa virtual de Maduro bombardea las redes para desinformar, RunRunEs, 28 Nov 2019, in: https://bit.ly/3qUa1jC [25 Feb 2021].
28 Organization of American States (OAS) 2019: Statement of the OAS General Secretariat, press release, 16 Oct 2019, in: https://bit.ly/3sqhYNJ [25 Feb 2021].
29 Slavin, Barbara / Healey, Jason 2013: Iran: How a Third Tier Cyber Power Can Still Threaten the United States, Atlantic Council Issue Brief, 29 Aug 2013, in: https://bit.ly/37Onr9f [25 Feb 2021].
30 Gross, Michael Joseph 2013: Silent War, Vanity Fair, Jul 2013, in: https://bit.ly/2ZRVby2 [6 Jan 2021].
31 Elswah, Mona / Howard, Philip N. / Narayanan, Vidya 2019: Iranian Digital Interference in the Arab World, COMPROP Data Memo, 3 Apr 2019, in: https://bit.ly/3pMIbEA [25 Feb 2021].
32 Carson, Austin 2019: Secret Wars. Covert Conflict in International Relations, Princeton.; Hofstetter, Yvonne 2019: Der unsichtbare Krieg. Wie die Digitalisierung Sicherheit und Stabilität in der Welt bedroht, Munich.