https://doi.org/10.18485/iipe_response2covid19.2021.ch11

CYBER DYPLOMACY AND THE COVID-19 – WHAT IS CYBER DIPLOMACY AND HOW WAS IT AFFECTED BY THE COVID-19 ERA?

Tal Pavel[1]

> "Diplomacy's lingua franca in the 19th century was French; in the 20th, it was English. The lingua franca of diplomacy in the 21st century is the mastery of digital tools and platforms"

Abstract: The COVID-19 pandemic has shaken our world since the beginning of 2020 and has had a wide impact on all aspects of life worldwide. Most of these consequences are international and transnational due to the wide scope of this pandemic, and international cooperation was often required even to assist and deal locally with its consequences. That happened mostly due to the limitations of a single country to deal with this pandemic and its far-reaching consequences, as well as the fact that among these were also a variety of cyberattacks against a large number of countries and a wide range of sectors, with an emphasis on the healthcare sector. Therefore, the place of diplomacy and an emphasis on cyber diplomacy is important in dealing with the consequences of the COVID-19 era and with cyberattacks that have occurred in its wake. Thus, this study analyses the extent of the impact of the COVID-19 pandemic on international cyber diplomacy, including the change in the conduct of relevant bodies and institutions, as well as cyber diplomacy decisions and policies to address cyberattacks related to this pandemic.

The study concludes that cyber diplomacy, which deals with both the digital aspects of diplomacy as well as the diplomatic management of cyber policies and events, was designed and modified as part of the effects of the COVID-19 pandemic. This includes a greater reliance on digital means of managing diplomatic work over physical encounters, as well as the need to use cyber

[1] PhD, The Academic College of Tel-Aviv Yaffo School of Information Systems, Israel, Talpv@mta.ac.il.

diplomacy to exercise international responsibility in this age of cyberattacks, particularly in the medical sector.

Keywords: COVID-19, cyber, diplomacy, EU, UN, Policy.

INTRODUCTION

Among the many changes brought about by the COVID-19 pandemic around the world since 2020 are the lockdowns imposed by many countries on their citizens in an attempt to reduce the scale of infection, which led to a transition even sharper than on normal days to an online remote-working model. Along with the many conveniences and opportunities, this approach has created numerous challenges, including those of information security and cybersecurity because a large number of employees have been sent to work from their homes, using unsecured work environments such as private email, internet and unsecured home computers, all this for connecting to work computers and connecting to sensitive files and data. Along with this, there has been a sharp and continuous increase throughout 2020 in cyberattacks, with an emphasis on the healthcare industry around the world. In this context, a variety of institutions were attacked, including critical infrastructure, especially hospitals, medical research institutions, drug manufacturing companies, as well as relevant government agencies by a variety of means: from disabling services by various means, including infidelity attacks, to attacks designed to steal data and important information related to and dealing with this pandemic.

The COVID-19 era demonstrates the impact of diverse global events, as well as their effects on cyberspace, and, therefore, the need for cyber diplomacy activities at the regional and international levels as part of the measures to address these crises, including the involvement of international organizations such as the UN, OSCE, G20 and the EU. This is to formulate new diplomatic norms and rules of cyber conduct during this and similar crises having a worldwide impact. All this is now happening while pointing accusing fingers at criminal elements as well as several state actors who are allegedly behind these attacks.

WHAT IS CYBER DIPLOMACY?

To examine the implementation of cyber diplomacy in the COVID-19 era, one must try and answer the question "What is cyber diplomacy?", and formulate its definition. Examination of various sources reveals that this is not a trivial matter since different terms refer to different areas of practice under these definitions, with the terms most often used: Cyber diplomacy, Digital diplomacy, e-diplomacy.

The affinity for the connection between new technology, the Internet, cyber and diplomacy can be divided into three stages: (1) Publications from the first decade of the 21st century addressing the two-way affinity between diplomacy and new technologies on the one hand and the Internet and the digital transformation of diplomacy on the other hand: their impact on goals, tools and diplomatic activity in the face of such diplomatic activity on the Internet. But all this is without addressing issues related to cyberspace. (2) With the beginning of the second decade of the 21st century and the transformation of cyberspace, its opportunities and threats, internationally and politically, these issues were addressed in the technical aspects of this space as external aspects of domestic policies, including developing cyber capabilities, improving government coordination and deepening cooperation with the private sector. (3) Later, the domain of cyber diplomacy moved from the local to the international level and gained recognition as a major issue in foreign policy due to many events, meetings and issues in cyberspace that required a diplomatic response.

All of these are reflected in the use of the various terms and in the change that has taken place in their usage over the years. Similar to the three steps described above, various researchers propose the following distinction. Digital diplomacy and e-diplomacy refer to the use of digital tools and methods for diplomatic purposes (e.g., the use of digital platforms and tools such as Big Data and data mining), including the use of digital means, such as social networks, by diplomats and foreign ministers. On the other hand, cyber diplomacy refers to the use of diplomatic tools and mindset to solve issues that arise in cyberspace (for example, Internet governance). With the increasing use of technologies on which cyberspace and the Internet are based, the need and importance of cybersecurity and the freedom of the Internet are also increasing. Several researchers have well defined the nature of cyber diplomacy, including "if the cyber dimension is the core reason for the diplomacy, it is cyber diplomacy", as well as the definition that cyber diplomacy constitutes diplomacy in the cyber domain and "the use of diplomatic resources and the performance of diplomatic functions to secure national interests in cyberspace".

The roots of cyber diplomacy are found in "standard" diplomacy. It is primarily state-led. However, it is a combination of two worlds: diplomatic-political and technological-cyber. It is a developmental stage in public diplomacy and is therefore also called public diplomacy 2.0. Thus, in recent years, a new role has been created called "cyber diplomats", who also constitute "cyber ambassadors" of their countries and deal with, among other things, the increasing politicization of cyberspace, for instance, the inclusion of cyber issues into policies dealing with internal and external security, critical infrastructure, and human rights. As well defined by Heli Tiirmaa-Klar, the ambassador of Estonia for cyber diplomacy, **"**as nuclear engineers do not represent states at the non-proliferation negotiations, likewise technology experts should not drive the issue of cyber diplomacy" and yet, "Like nuclear-era diplomats, they should understand the effects of destructive cyber tools and how critical infrastructures could be used for paralysing states in future conflict"**.** This is also because traditional diplomacy is not necessarily appropriate for the type of diplomacy that has changed in a world where cyberspace is a powerful weapon between countries, which requires relevant diplomatic activity to build trust, prevent escalation or misattribution of cyberattacks. This is in addition to activities to create norms, binding and non-binding, for the responsible behaviour of a country in cyberspace through the activities of bilateral, multilateral and regional bodies. Alongside official and government diplomacy, there is the activity of non-state actors, including companies and NGOs, mainly because about 80-90% of critical cyber assets belong to the private sector. The vulnerabilities of those assets and the consequences of harming them should be considered too. These players all work together on issues such as multilateralism, security, capacity building, cybercrime warfare, Internet governance, freedom of expression and online human rights, cyber espionage, regulation of cyber warfare, and issues that form the basis of foreign relations in the cyber domain, with different players emphasizing different aspects. All this is to create a global consensus on norms of responsible state behaviour in cyberspace and with an emphasis on global norms for this purpose over the individual ones.. These are reflected in national strategy documents in the field of cyberspace, including cyber security, cybercrime, trust-building, Internet freedom, and Internet governance. In this context, the document titled "US International Strategy for Cyberspace", which will be mentioned further on, and published in 2011 by the Obama administration, became the world's first strategy document dealing entirely with international aspects of cyber issues. It outlined, for the first time, a clear strategy for the use of diplomatic tools and resources to achieve goals related to cyberspace.

From the variety of sources, it can be learned that the affinity between the world of diplomacy and the digital world developed alongside the development of the digital world. Its great importance has begun to influence more and more countries, their policies, and conduct. Thus, initially, when affinity focused on the use of the digital world and social networks as a means of managing and promoting diplomacy, the prevalent use was e-diplomacy as well as digital diplomacy. However, as the importance of cyberspace and the awareness of its many and varied effects on the life of a modern country increased, so did the use of the term cyber diplomacy, which describes the shift from using the digital world for diplomatic needs to using the diplomatic world to meet cyberspace needs. So, all in all, it can be said that in "digital diplomacy", the digital world is a tool for the use of diplomacy, while in "cyber diplomacy", diplomacy is a tool for solving threats and problems in cyberspace as well as securing national interests in that space.

CYBERATTACKS DURING THE COVID-19 ERA

The COVID-19 era has created a wide range of changes, challenges and threats for all of humanity in every country and sector. This includes a sharp increase in cyberattacks during 2020, one that is directly related to the pandemic and its consequences, which can be examined in several aspects: (1) the type of attack, (2) the attacked, and (3) the attacker.

TYPES OF ATTACKS

When analysing the types of cyberattacks that occurred during the COVID-19 pandemic, it seems that these were many and varied types that were carried out by a variety of attackers who took advantage of several factors: (1) The transition to the remote working model due to the lockdowns imposed by many countries in which workers were sent to work from home using unsecured means, including email, personal computers and home Internet connections, to connect to work computers and access sensitive files and information; (2) a lack of appropriate awareness and sufficient training for these employees regarding the information security dangers that exist in the remote working model, as well as the way to deal with these threats; (3) the uncertainty, fear and apprehension of the unknown among the entire population, with an emphasis on layoffs or a reduction in the wage level among workers; (4) The need for information on the pandemic, its consequences and the means to confront it, including appropriate equipment and the development of vaccines. In this context, a variety of malicious attacks of cybercrime were carried out for many reasons, which included: ransomware ; various scams, including those allegedly related to financial aid and grants, and trafficking in counterfeit medical equipment ; data theft, leaking and trading ; distribution of malware ; malicious emails and phishing ; fake news campaigns and the dissemination of conspiracy theories, known as Infodemic; theft of intellectual property, most often associated with dealing with the pandemic and developing a vaccine. In all of these, there has been an unprecedented increase worldwide over the entire year 2020, as reported by a variety of sources and publications.

THE ATTACKED

In many cases, the target of various attacks was organizations and their employees who, due to the lockdowns during the COVID-19 pandemic, moved to work in a remote working model. Indeed, a variety of publications report a sharp increase in such attacks, as well as in the sense of insecurity of employees working from home and the dependence on various third-party suppliers external to their organizations. At the same time, the healthcare sector has been the most attacked since the beginning of 2020. These attacks were mostly executed by state actors, to the point when, for example, the International Committee of the Red Cross called for them to stop attacking this sector.

THE ATTACKER

Along with criminals who took advantage of the changes and security breaches created, especially in the remote working era (Associated Press, 2020), various countries have been accused of involvement in carrying out cyberattacks around the world against laboratories, research institutes, hospitals, drug makers, universities in search of information, equipment, medicines, vaccines and everything else necessary to help them deal with this pandemic.

CYBER DIPLOMACY DURING THE COVID-19 ERA

Analysis of the various publications and studies on cyber diplomacy in the COVID-19 era reveals that this field may have changed more than most professions during this pandemic. The reference is indeed divided into two aspects of the essence of cyber diplomacy: (1) The cyber challenges posed by the pandemic and its consequences, (2) the use of digital tools, which have become more common due to the limitations posed by the pandemic, for improving diplomacy work.

The main characteristic of the COVID-19 era is the digitalization of economies and societies. It has brought a huge increase in the use of digital services to create online communication for various needs in a focused manner and as part of an overall policy, including teaching, work (individual or group), banking, health, along with an online alternative to physical meetings. It has created a host of threats and dangers to information security, privacy and even critical infrastructure on the part of a variety of players. It has also heightened mistrust and suspicion between different countries in light of various online attacks and hostile actions that some countries have committed during this pandemic. Among other things, countries aim to advance their various national interests as well as foreign policy goals, or even cyber revenge on the political or military activities of other countries in this era. Various researchers point out that the fog that accompanies these operations, which were below the threshold of armed conflict even before the COVID-19 era and even more so during this period, creates more grounds for conflicts, which requires regional and international cyber diplomacy efforts to create a more secure environment, even in cyber aspects, while emphasizing the activities of smaller countries.

In addition, various researchers and experts address the changes that have taken place in the work of diplomacy in this age, using digital platforms that allow for greater ease, benefit and efficiency, without cost constraints, travel expenses, logistics and time constraints, while improving verbal and written communication skills. This includes the possibility of expanding the activity to a diverse international audience, with the participation of senior officials, linking many countries, in a wide range of fields and sectors. An example of this is the marine biological diversity of areas beyond national jurisdiction (BBNJ), in which regional and international discussions were held, with the participation of NGOs together with several governments, as well as the conduction of surveys and studies. These moved to an online environment instead of the physical one, with a drastic drop in the rate of face-to-face meetings, as opposed to a significant increase in the use of email, virtual meetings and instant messaging applications. This is in addition to the expected effect of the transition from physical meetings to the use of online means on the results of BBNJ negotiations and the assumption of NGOs that such online negotiations will be more inclusive in the face of state players who have rejected this assumption. Various researchers and experts expect that even with the end of this crisis, the intensified digital use during the COVID-19 crisis will be a lesson for diplomats to "think digitally" and improve their tools and knowledge on this matter, so they can better help their countries to deal with future global crises. However, there are many concerns, including the main claim that online communication is not a substitute for physical presence and the personal aspect of diplomacy, for example, holding the UN votes by sending e-mails over online voting because "WhatsApp chats cannot replace the corridor diplomacy for getting a consensus". This is alongside concerns about the impact and consequences of postponing various conferences in 2020 and the burden that will be created in 2021 mainly on small and developing countries with fewer experts and representatives, as well as the cuts these have experienced in diplomatic services. In addition, various diplomats and experts point out that digital solutions do not replace bilateral meetings, or meetings on the sidelines of conferences and events, addressing the need for technologically secure communication for sensitive discussions, as well as the need for appropriate communication capabilities in small and developing countries. In this context, it was noted that in one of the UN discussions of the Warsaw International Mechanism, the Sudanese representative could not participate due to low bandwidth, which prevented continuous and quality communication. Besides, some governments have banned the use of various platforms, including Zoom, for security and confidentiality reasons. In addition, some point out that this pandemic has revealed the growing dissatisfaction with multilateral governance and the ongoing recognition that the existing system and the multitude of international organizations that are part of it do not fully reflect the strategic reality, are unable to achieve their goals, appear more political than practical, and have become inefficient and even corrupt. Those online meetings will save the many costs involved in having physical meetings, especially in the era of budget cuts as part of the plague consequences.

At the same time, one of the interesting effects of the COVID-19 pandemic on global diplomacy is the so-called "Corona Diplomacy", which is using the pandemic to promote the political and sometimes even personal interests of a country's leader. This is done, mainly by China, Turkey, Qatar and Cuba, by sending medical staff and appropriate equipment to promote the status of the offering country among the countries of the region and the international community. The claim is that such aid is nothing new, but due to the pandemic and its devastating international consequences, such aid is gaining widespread international exposure and recognition. This is in addition to diplomatic activities, such as consular assistance to those who are stuck abroad, assistance with procurement performed for medical equipment, as well as international cooperation in the search for a vaccine for the pandemic.

When examining the effects of COVID-19 on cyber diplomacy, one can see the beginning of an important trend in which countries update official policy documents dealing with diplomacy and cyberspace to address the changes that the COVID-19 pandemic has posed to cyber diplomacy around the world. An example of this can be found in an official document of the Estonian government called "Estonian Foreign Policy Strategy 2030" which also addresses these implications:

> "An example of the materialisation of such threats is the COVID-19 pandemic (2020), which has caused a deep global crisis, a prolonged duration of which is likely to have serious consequences not only for healthcare and the economy but also for security. The short-term effects of the crisis manifest themselves, among other things, in global rivalries in handling the pandemic and pressures on social and healthcare systems (which may affect the internal functioning of countries), and have had an impact on trust and cooperation between countries. The system of international relations and cooperation based on the current rules may change significantly as a result of the crisis. The pandemic highlighted in particular the importance of international cooperation in tackling global challenges".

Another expression of the spirit of the period can be found in the document "Cybersecurity Strategy of Ukraine, 2021-2025", in which, among the four challenges facing Ukraine in the field of cybersecurity, the last challenge is

> "impact on economic activity and social behaviour of the spread of the COVID-19 pandemic, which led to the rapid transformation and organization of a significant segment of public relations remotely with the widespread use of electronic services and information and communication systems. This has exacerbated the threat of violations of citizens' rights when using cyberspace.".

CONCLUSIONS

The era of the COVID-19 pandemic has created a wide range of changes around the world, challenges and opportunities, some that will pass with the retreat of the pandemic, and some that are likely to stay with us for a long time and even forever affect certain aspects of our lives as individuals, organizations and countries. It seems that, as in many areas affected by COVID-19, diplomacy will not return to what it was. Experts indeed agree that this pandemic will have long-term implications for diplomacy and multilateral governance, with the need to find the golden path between adopting the changes and going back to the pattern of a diplomatic routine. In this context, the field of cyber diplomacy seems to be changing in two aspects of its activity: (1) expanding the use of various online platforms to carry out a variety of activities involving diplomatic work, including multi-participant multilateral discussions, as well as ongoing diplomatic activity; (2) deepening the use of diplomacy to manage regional and international cyber events and crises, as well as deepening international activity to create responsible rules of conduct on the part of countries in relation to cyberspace activities, in times of peace and especially in times of crises. These changes occur both at the international level in the activities of various international organizations and at the level of a single country. They include local activities both in aspects of online diplomatic activity and also on issues such as the exploitation of the pandemic for the purpose of promoting various state interests. They go as far as to update policy documents in the fields of foreign and cyber relations so that they express the pandemic and its effects in the field of cyber diplomacy.

As this era is still upon us and at various stages of development, it is not possible to estimate its full extent and intensity of its consequences and effects in general and in the field of cyber diplomacy in particular. Thus, this study is an analysis of the existing situation when future research will be able to examine things in a broader scope and over a longer period and provide a broader and fuller picture of the effect of the COVID-19 pandemic over cyber diplomacy.

REFERENCES

Abrams, L. (2020, April 13). Over 500,000 Zoom accounts sold on hacker forums, the dark web. BeepingComputer, retrieved from https://www.bleepingcomputer.com/news/security/over-500-000-zoom-accounts-sold-on-hacker-forums-the-dark-web/. Accessed 15 May 2021.

Adams, K. (2020, October 12). The 10 healthcare organizations most affected by cyberattacks in 2020. Becker's Healthcare, retrieved from https://www.beckershospitalreview.com/cybersecurity/the-10-healthcare-organizations-most-affected-by-cyberattacks-in-2020.html. Accessed 15 May 2021.

Addison, K. (2020, April 16). Threat Intelligence Briefing: Surging Spam and Impersonation Attacks Drive Increasing Coronavirus Cyber Threats. Mimecast Blog, retrieved from https://www.mimecast.com/blog/threat-intelligence-briefing-surging-spam-impersonations-drive-increasing-coronavirus-cyber-threats/. Accessed 15 May 2021.

Attatfa, A., Renaud, K., & de Paoli, S. (2020). Cyber diplomacy: A systematic literature review. *Procedia Computer Science*, 176, pp. 60–69. https://doi.org/10.1016/j.procs.2020.08.007

Barrinha, Andre. (2020, June 10). The Emergence of Cyber Diplomacy in an Increasingly Post-Liberal Cyberspace. Council on Foreign Policy, retrieved from https://www.cfr.org/blog/emergence-cyber-diplomacy-increasingly-post-liberal-cyberspace. Accessed 5 June 2021.

Barrinha, André, & Renard, T. (2017). Cyber-diplomacy: the making of an international society in the digital age. *Global Affairs*, 3(4–5), pp. 353–364. https://doi.org/10.1080/23340460.2017.1414924.

Bartolome, G. D. (2021, July 6). The hybrid future of diplomacy. Washington Diplomat, retrieved from https://washdiplomat.com/the-hybrid-future-of-future-diplomacy/. Accessed 5 June 2021.

Bashir, N., Liakos, C., Seo, Y., Jeong, S., & Watson, A. (2020, November 27). North Korean hackers suspected of targeting vaccine maker AstraZeneca in cyberattack. CNN, retrieved from https://edition.cnn.com/2020/11/27/asia/north-korea-astrazeneca-suspected-cyberattack-intl/index.html. Accessed 20 June 2021.

Bhavani, D. K. (2021, June 2). Beware Coronavirus-themed cyber-attacks, urges McAfee. The Hindu, retrieved from https://www.thehindu.com/sci-tech/technology/internet/mcafee-2021-consumer-mindset-report-covid19-cybersecurity-internet-habits-india/article34699465.ece. Accessed 5 June 2021.

Brewster, T. (2020, March 18). An 'Unprecedented' Wave of Coronavirus Scams Is Coming, U.S. Attorney Warns. Forbes, retrieved from https://www.forbes.com/sites/thomasbrewster/2020/03/18/how-americas-cyber-defenders-are-preparing-to-save-you-from-an-unprecedented-wave-of-coronavirus-scams/?sh=4d146507a74a. Accessed 1 July 2021.

Canter, L. (2020, April 29). Coronavirus: Half of remote workers "victims of cybercrime." Yahoo! News, retrieved from https://uk.news.yahoo.com/coronavirus-half-of-remote-workers-victims-of-cybercrime-144200532.html?guccounter=1. Accessed 20 June 2021.

Cempaka Timur, F. G. (2017). The Rise of Cyber Diplomacy ASEAN's Perspective in Cyber Security. *KnE Social Sciences*, 2(4), pp. 244–250. https://doi.org/10.18502/kss.v2i4.893.

Christian. (2019, November 11). Digital Diplomacy vs Cyber Diplomacy. Association of Accredited Public Policy Advocates to the European Union, retrieved from http://www.aalep.eu/digital-diplomacy-vs-cyber-diplomacy. Accessed 20 June 2021.

Deeba, A. (2020, May 8). Hackers hit Europe's largest healthcare provider with Snake ransomware. HackRead, retrieved from https://www.hackread.com/hackers-hit-europe-healthcare-provider-snake-ransomware/. Accessed 1 July 2021.

Desai, D. (2020, April 23). 30,000 Percent Increase in COVID-19-Themed Attacks | Zscaler. Zscaler Blog, retrieved from https://www.zscaler.com/blogs/security-research/30000-percent-increase-covid-19-themed-attacks. Accessed 1 July 2021.

ENISA. (2020, May 11). Cybersecurity in the healthcare sector during COVID-19 pandemic, retrieved from https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-healthcare-sector-during-covid-19-pandemic. Accessed 5 June 2021.

E&T. (2020, April 17). Hacking against corporations soars as staff work from home. E&T Magazine, retrieved from https://eandt.theiet.org/content/articles/2020/04/hacking-against-corporations-surges-as-people-work-from-home/. Accessed 1 July 2021.

Europol. (2020, March 21). Rise of fake 'corona cures' revealed in global counterfeit medicine operation, retrieved from https://www.europol.europa.eu/newsroom/news/rise-of-fake-%E2%80%98corona-cures%E2%80%99-revealed-in-global-counterfeit-medicine-operation. Accessed 20 June 2021.

Faizal bin Abdul Rahman, M. (2020, June 17). COVID-19 and Future of Cyber Conflict. The Diplomat, retrieved from https://thediplomat.com/2020/07/covid-19-and-future-of-cyber-conflict/. Accessed 2 May 2021.

Federal Foreign Office. (2020, November 19). EU Cyber Diplomacy – working together for a free and secure cyberspace, retrieved from https://www.auswaertiges-amt.de/en/aussenpolitik/themen/eu-cyber-non-paper/2418984. Accessed 5 June 2021.

Federal Trade Commission. (2020, March 31). FTC Data Shows Jump in Coronavirus-related Complaints from Consumers. Federal Trade Commission, retrieved from https://www.ftc.gov/news-events/press-releases/2020/03/ftc-data-shows-jump-coronavirus-related-complaints-consumers. Accessed 2 May 2021.

Fidler, D. P. (2020, March 30). Cybersecurity in the Time of COVID-19, retrieved from https://www.cfr.org/blog/cybersecurity-time-covid-19. Accessed 5 June 2021.

Fleming, S. (2020, May 6). Surge in security concerns due to remote working during COVID-19 crisis. Journey Notes, retrieved from https://blog.barracuda.com/2020/05/06/surge-in-security-concerns-due-to-remote-working-during-covid-19-crisis/. Accessed 5 June 2021.

Freeman, C. (2021, April 29). Diplomacy has changed more than most professions during the pandemic. The Economist, retrieved from https://www.economist.com/international/2021/04/29/diplomacy-has-changed-more-than-most-professions-during-the-pandemic. Accessed 2 May 2021.

Goodwin, B. (2020, March 22). Cyber gangsters hit UK medical firm poised for work on coronavirus with Maze ransomware attack. Computer Weekly, retrieved from https://www.computerweekly.com/news/252480425/Cyber-gangsters-hit-UK-medical-research-lorganisation-poised-for-work-on-Coronavirus. Accessed 5 June 2021.

Grierson, J., & Devlin, H. (2020, May 3). Hostile states trying to steal coronavirus research, says UK agency. The Guardian, retrieved from https://www.theguardian.com/world/2020/may/03/hostile-states-trying-to-steal-coronavirus-research-says-uk-agency. Accessed 5 June 2021.

Gülmez, S. B. (2020). 5th International EMI Entrepreneurship and Social Sciences Congress. The Impact of COVID-19 Pandemic on Diplomacy, pp. 367–378, retrieved from https://www.researchgate.net/publication/344402901. Accessed 1 July 2021.

Heath, R. (2020, April 16). For global diplomats, Zoom is not like being in the room. POLITICO, retrieved from https://www.politico.com/news/2020/04/16/zoom-diplomacy-coronavirus-188811. Accessed 1 July 2021.

Hocking, B., & Melissen, J. (2015). Diplomacy in the Digital Age, retrieved from https://www.clingendael.org/sites/default/files/pdfs/Digital_Diplomacy_in_the_Digital%20Age_Clingendael_July2015.pdf. Accessed 1 July 2021.

Hone, K. (2020, December 23). WebDebate #44: Diplomacy during COVID-19 in developing countries. Diplo, retrieved from https://www.diplomacy.edu/blog/webdebate-44-summary-diplomacy-times-covid-19-experience-developing-countries. Accessed 1 July 2021.

International Committee of the Red Cross. (2020, May 25). Governments must stop cyber attacks on health care, retrieved from https://www.icrc.org/en/document/governments-work-together-stop-cyber-attacks-health-care. Accessed 1 July 2021.

Internet Crime Complaint Center (IC3). (2020, April 1). Cyber Actors Take Advantage of COVID-19 Pandemic to Exploit Increased Use of Virtual Environments, retrieved from https://www.ic3.gov/Media/Y2020/PSA200401. Accessed 5 June 2021.

INTERPOL. (2020, August 4). INTERPOL report shows alarming rate of cyberattacks during COVID-19. INTERPOL, retrieved from https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19. Accessed 2 May 2021.

Klebnikov, S. (2020, May 8). Gilead Sciences Targeted By Hackers Linked To Iran: Report. Forbes, retrieved from https://www.forbes.com/sites/sergeiklebnikov/2020/05/08/gilead-sciences-targeted-by-iranian-linked-hackers-report/?sh=42ff718713db#2dd1cfb013db. Accessed 5 June 2021.

Krebs, B. (2020, March 12). Live Coronavirus Map Used to Spread Malware. Krebs on Security, retrieved from https://krebsonsecurity.com/2020/03/live-coronavirus-map-used-to-spread-malware/. Accessed 2 May 2021.

Kumaran, N., & Lugani, S. (2020, April 16). Protecting against cyber threats during COVID-19 and beyond. Google Cloud Blog, retrieved from https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond. Accessed 2 May 2021.

Labott, E. (n.d.). Redefining Diplomacy in the Wake of the COVID-19 Pandemic Produced and edited by The Meridian Center for Diplomatic Engagement. The Meridian Center for Diplomatic Engagement, pp. 1–15, retrieved from https://www.meridian.org/wp-content/uploads/2020/10/Redefining-Diplomacy-Report-v3.pdf. Accessed 20 June 2021.

Liu, R., Jarmuzek, T., & Vasilenko, R. (2020, May 20). Phishing in The Time of Pandemic. Lastline, retrieved from https://www.lastline.com/labsblog/phishing-in-the-time-of-pandemic/. Accessed 2 May 2021.

McBride, S. (2020, May 14). Why The Largest Cyberattack in History Could Happen Within Six Months. Forbes, retrieved from https://www.forbes.com/sites

/stephenmcbride1/2020/05/14/why-the-largest-cyberattack-in-history-will-happen-within-six-months/?sh=566a6953577c. Accessed 20 June 2021.

McDougal, G. (2020, May 12). Coronavirus cyber-attacks update: beware of the phish. Check Point, retrieved from https://blog.checkpoint.com/2020/05/12/coronavirus-cyber-attacks-update-beware-of-the-phish/amp/. Accessed 2 May 2021.

Meyer, P. (2015). Seizing the Diplomatic Initiative to Control Cyber Conflict. *Simons Papers in Security and Development*, pp. 1–20. https://doi.org/10.1080/0163660X.2015.1064709

Miller, M. (2020, April 16). FBI sees spike in cyber crime reports during coronavirus pandemic. The Hill, retrieved from https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic. Accessed 2 May 2021.

Minchev, Z. (2021). Disruptive Effects of New Pandemic Age to Shifted Cyber Diplomacy due to Multilateral Mixed Transformation. International Journal of Cyber Diplomacy, retrieved from https://www.researchgate.net/publication/351776173. Accessed 15 May 2021.

Ministry of Foreign Affairs. (2020). Estonian Foreign Policy Strategy 2030, retrieved from https://vm.ee/sites/default/files/Estonia_for_UN/Rasmus/estonian_foreign_policy_strategy_2030_final.pdf. Accessed 15 May 2021.

Moret, E., & Pawlak, P. (2017). The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?, retrieved from https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2024%20Cyber%20sanctions.pdf. Accessed 15 May 2021.

Muncaster, P. (2020, March 26). #COVID19 Fears Drive Phishing Emails Up 667% in Under a Month- Infosecurity Magazine. Infosecurity Magazine, retrieved from https://www.infosecurity-magazine.com/news/covid19-drive-phishing-emails-667/. Accessed 5 June 2021.

National Security and Defense Council of Ukraine. (2021, March 4). The working group at the NCCC at the NSDC of Ukraine approved the draft Cybersecurity Strategy of Ukraine, retrieved from https://www.rnbo.gov.ua/en/Diialnist/4838.html. Accessed 5 June 2021.

Norwich University Online. (2020, September 30). The Increasing Need for Cyber Diplomacy, retrieved from https://online.norwich.edu/academic-programs/resources/increasing-need-cyber-diplomacy. Accessed 5 June 2021.

Ortega, A. (2020, March 31). Infodemic and mediademic. Elcano, retrieved from https://blog.realinstitutoelcano.org/en/infodemic-and-mediademic/. Accessed 2 May 2021.

Osborne, S. (2020, May 3). Iran and Russia launch cyber attacks on universities desperately searching for COVID cure. Express, retrieved from https://www.express.co.uk/news/uk/1277156/Iran-news-coronavirus-vaccine-uk-universities-cyber-attack-crime-russia. Accessed 2 May 2021.

Paganini, P. (2020a, March 14). One of the major COVID-19 testing laboratories in Czech hit by cyberattack. Security Affairs, retrieved from https://security affairs.co/wordpress/99598/hacking/covid-19-czech-hospital-hit-cyberattack.html. Accessed 2 May 2021.

Paganini, P. (2020b, April 14). Crooks target Healthcare facilities involved in Coronavirus containment with Ransomware. Security Affairs, retrieved from https://securityaffairs.co/wordpress/101571/malware/healthcare-coronavirus-ransomware-attacks.html. Accessed 18 June 2021.

Painter, C. (2018, June). Diplomacy in Cyberspace. The Foreign Service Journal, retrieved from https://www.afsa.org/diplomacy-cyberspace. Accessed 18 June 2021.

Panda, A. (2020, April 24). Offensive Cyber Capabilities and Public Health Intelligence: Vietnam, APT32, and COVID-19 – The Diplomat. The Diplomat, retrieved from https://thediplomat.com/2020/04/offensive-cyber-capabilities-and-public-health-intelligence-vietnam-apt32-and-covid-19/. Accessed 20 June 2021.

Riodan, S. (2016, May 12). Cyber Diplomacy vs. Digital Diplomacy: A Terminological Distinction. USC Center on Public Diplomacy, retrieved from https://usc publicdiplomacy.org/blog/cyber-diplomacy-vs-digital-diplomacy-terminological-distinction. Accessed 20 June 2021.

Robertson, J. (2020, August 18). Diplomacy and global governance after Covid 19: Prepare for change. The Interpreter, retrieved from https://www.lowy institute.org/the-interpreter/diplomacy-and-global-governance-after-covid-19-prepare-change. Accessed 18 June 2021.

Skybox Security. (2020, July 21). COVID-19 Pandemic Sparks 72% Ransomware Growth, Mobile Vulnerabilities Grow 50%. Skybox Security, retrieved from https://www.prnewswire.com/in/news-releases/covid-19-pandemic-sparks-72-ransomware-growth-mobile-vulnerabilities-grow-50—817268901.html. Accessed 20 June 2021.

Sobers, B. (2021, January 29). 134 Cybersecurity Statistics and Trends for 2021. Varonis, retrieved from https://www.varonis.com/blog/cybersecurity-statistics/. Accessed 15 May 2021.

Steed, D. (2020, July 14). COVID-19: reaffirming cyber as a 21st century geopolitical battleground. Elcano, retrieved from http://www.realinstitutoelcano.org/

wps/portal/rielcano_en/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_in/zonas_in/ari94-2020-steed-covid-19-reaffirming-cyber-as-21st-century-geopolitical-battleground. Accessed 15 May 2021.

Stojanovska-Stefanova, A., & Magdincheva-Shopova, M. (2020). Digital Diplomacy as a Form of Change Management in International Relations in Times of COVID-19. *KNOWLEDGE - International Journal*, 41(5), pp. 1069–1074, retrieved from http://eprints.ugd.edu.mk/26752/1/KIJ%2C%20Vol.%2041.5-pages.pdf. Accessed 15 May 2021.

Stubbs, J., & Bing, C. (2020, May 8). Exclusive: Iran-linked hackers recently targeted coronavirus drugmaker Gilead - sources. Reuters, retrieved from https://www.reuters.com/article/us-healthcare-coronavirus-gilead-iran-ex-idUSKBN22K2EV. Accessed 15 May 2021.

The White House. (2011). International Strategy for Cyberspace, retrieved from https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. Accessed 2 May 2021.

TheCyberDiplomat. (2019, October 12). Cyber Diplomacy: Governance Beyond Government, retrieved from https://medium.com/@cyberdiplomacy/cyber-diplomacy-governance-beyond-government-e8b92effff8f. Accessed 2 May 2021.

Tiirmaa-Klaar, H. (2013). Cyber Diplomacy: Agenda, Challenges and Mission. In Peacetime Regime for State Activities in Cyberspace (pp. 509–531). NATO Cooperative Cyber Defence Centre of Excellence, retrieved from https://d1wqtxts1xzle7.cloudfront.net/40986873/Peacetime-Regime_for_state_activities_in_cyberspace.pdf?1452115842=&response-content-disposition=inline%3B+filename%3DPeacetime_Regime_for_state_activities_in.pdf&Expires=1623317597&Signature=fHglzI5vihZK5jr6ROInihNau3mxxQED2grF7bnVJ1mvylZuqM0LMYNiBfJff9bMcHcUYu5DKEqJznSfe6Mf9Cfit1giNjYC0FEPfbWlbV6EpjzavvYLa39m-GA8u4qwzTcoANmQrudvYA8seix3EQXLsZHtWVaMuaPn-KZo6mcBsqskmX~MTEpSNX7aTAmbfYDBTCQoavy3I3URnWOYeNWpMXc~t8TpxyA5ha~-Z4L3PaODOfl-ROP3IZ94Ge7fDPy9vtTJQGG46K7ZOKwI25-UJMrN1lMrs2X34agVVihCaFojsU5-PXZeTOLcfUbBAxRQVhvTKTPCySprZBmmww__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA. Accessed 15 May 2021.

Torres, M., & Riordan, S. (2020). The cyber diplomacy of constructing norms in cyberspace, retrieved from https://www.g20-insights.org/policy_briefs/the-cyber-diplomacy-of-constructing-norms-in-cyberspace/. Accessed 15 May 2021.

Toth, S. (2020, May 26). How COVID-19 will impact future cyberdiplomacy. OSCE, retrieved from https://www.osce.org/blog/how-COVID19-will-impact-future-cyberdiplomacy. Accessed 20 June 2021.

Vadrot, A. B. M., Langlet, A., Tessnow-Von Wysocki, I., Tolochko, P., Brogat, E., & Ruiz-Rodríguez, S. C. (2021). Marine Biodiversity Negotiations During COVID-19: A New Role for Digital Diplomacy? under a Creative Commons Attribution 4.0 International (CC BY 4.0) license. https://doi.org/10.1162/glep_a_00605

van der Meulen, R. (2020, April 24). Gartner Says 52% of Legal & Compliance Leaders Are Concerned About Third-Party Cybersecurity Risk Since COVID-19. Gartner, retrieved from https://www.gartner.com/en/newsroom/press-releases/2020-04-24-gartner-says-52-percent-of-legal-and-compliance-leaders-are-concerned-about-third-party-cybersecurity-risk-rince-covid-19. Accessed 20 June 2021.

Vijayan, J. (2020, September 15). More Cyberattacks in the First Half of 2020 Than in... Dark Reading, retrieved from https://www.darkreading.com/attacks-breaches/more-cyberattacks-in-the-first-half-of-2020-than-in-all-of-2019/d/d-id/1338926. Accessed 20 June 2021.

Waqas. (2020, May 10). Researchers detected 400 million malware infections in April 2020. HackRead, retrieved from https://www.hackread.com/400-million-malware-infection-in-april-2020/. Accessed 20 June 2021.

WHO. (2020, April 23). WHO reports fivefold increase in cyber attacks, urges vigilance, retrieved from https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance. Accessed 20 June 2021.

Wiesel, T. (2020). Keep an Eye on North Korean Cyber-Crime as the COVID-19 Spreads. Pacific Forum- Homolulu, retrieved from https://pacforum.org/wp-content/uploads/2020/03/20200317_PacNet_13.pdf. Accessed 15 May 2021.

Williams, S. (2020, October 2). Cyberattacks up 400% compared to pre-COVID-19 levels. Security Brief, retrieved from https://securitybrief.eu/story/cyberattacks-up-400-compared-to-pre-covid-19-levels. Accessed 15 May 2021.