UA: UKRAINE ANALYTICA

Issue 2 (20), 2020

ANNIVERSARY

5 YEARS

- CONVENTIONAL DIPLOMACY
- DIGITAL DIPLOMACY
- QUARANTINE DIPLOMACY

UA: UKRAINE ANALYTICA

Issue 2 (20), 2020

Diplomacy

Editors
Dr. Hanna Shelest
Dr. Mykola Kapitonenko

Publisher:
Published by NGO "Promotion of Intercultural Cooperation" (Ukraine), Centre of International Studies (Ukraine), with the financial support of the Representation of the Friedrich Ebert Foundation in Ukraine, the Black Sea Trust.

UA: Ukraine Analytica is the first Ukrainian analytical journal in English on International Relations, Politics and Economics. The journal is aimed for experts, diplomats, academics, students interested in the international relations and Ukraine in particular.

Contacts:
website: http://ukraine-analytica.org/
e-mail: Ukraine_analytica@ukr.net
Facebook: https://www.facebook.com/ukraineanalytica
Twitter: https://twitter.com/UA_Analytica

ISSN 2518-7481

500 copies

BOARD OF ADVISERS

TABLE OF CONTENTS

CYBER DIPLOMACY: AN INTANGIBLE REALITY OR A FAIT ACCOMPLI?

Dr. Olga Rusova
Hennadii Udovenko Diplomatic Academy of Ukraine

A constantly changing international environment and a fast-paced advancement of information and communications technologies (ICTs) essentially modify the traditional ways of diplomacy. In the digital age, the use of e-tools has become a daily routine for diplomats, and the developments in the cyber realm define the global political agenda, transforming the mechanisms of multilateral cooperation. Meanwhile, the digitalisation of diplomatic interactions is intrinsically tied with cyber risks. The lack of a solid legal framework for regulation of the virtual space inevitably leads to conflicts. This article highlights new features that cyber diplomacy brings into international relations, raising the issue of online security, appropriate response to cyberattacks, and a right for self-defence.

Theoretical Background and Case Studies

For many centuries, diplomacy has been a privileged kind of statecraft in the spotlight with nation-states and political elites. But ever since information and communications technologies (ICTs) began to play a crucial role in guiding public opinion, diplomacy seems to have been simplified through the use of Facebook, Twitter, Instagram, or YouTube for communication with a vast audience. The need to integrate digital technologies into the diplomatic process gave way to cyber diplomacy. States tend to adopt broad strategies for addressing various issues and use wide networks of ICTs to express their current views and ideas about the future. They incorporate virtual reality into their foreign policies and use cyber diplomacy to promote their concept of an international society.[1] However, before continuing with the analysis of cyber diplomacy implications, I would propose first to sort out the sometimes overlapping terms such as *public, digital*, and *cyber diplomacy*. Clear definitions may be useful in order to avoid confusions and misunderstandings.

Let's start with *public diplomacy* and its direct link to the soft power of states with a wide range of determinants, among which are political values, culture, foreign policy, and, of course, public diplomacy. It is focused on nation branding and at the same time is a part of a national identity. This is a strategy of a government aiming to shape public opinion and attitudes to its country abroad, which could affect the foreign policy course of other states. Public diplomacy puts an emphasis on two-way communication and open dialogue.

1 F. T. Burroughs, *The Diplomatic Tower of Babel,* "Public Diplomacy Magazine" (University of South California, Center for Public Diplomacy), 22, 2019, p. 52.

As for *digital diplomacy*, it can be viewed as an extension of soft power and public diplomacy, and is equipped with a new digital toolkit and techniques. It calls attention to a broader perspective of the role of digital technology in diplomacy as not only an instrument or medium of communication but also as a different mode of thinking about and practicing diplomacy.[2]

And finally, to distinguish between digital and *cyber diplomacy,* the latter puts stress on the use of diplomatic tools, and the diplomatic mindset, to resolve issues arising in cyberspace.[3] Of course, the number of those matters can be enormous. They vary from completely peaceful initiatives such as multilateral forums or global climate campaigns to highly damaging ones such as propaganda and espionage.

However, the primary concern here is not only to draw attention to the wording but also to dwell on the practical examples of cyber diplomacy in action. In this regard, the case of Kosovo is a notable example. Despite the fact that Kosovo declared its independence from Serbia in 2008 and has been recognised by many countries, including three permanent members of the UN Security Council (the UK, France, and the US), for most of the EU states and Canada, it still remains an online limbo. To date the Internet Corporation for Assigned Names and Numbers (ICANN) has been refusing to grant Kosovo its own country code top-level domain (ccTLD). For this reason, Kosovo has to run its internet traffic either under "foreign flags" or route it through third countries. Under these circumstances, a ccTLD is not just a symbolic indicator of independence. Through the existence of private ccTLDs, Kosovo would control an essential part of their information and technological infrastructure that can affect telecommunications, power grids, banking, and electronic surveillance.

National governments recognise the internet domain as a component of their sovereignty. Furthermore, through its domain, Kosovo can lobby for recognition of the country.[4] On the one hand, this situation leaves little room for manoeuvre on the global stage; on the other hand, it stimulates the use of its soft power and focus on the promotion of Kosovo's culture and history by means of online tools. In this regard, a matter of nation branding is a crucial problem, because foreigners view the country as associated with corruption, social unrest, and territorial disputes.

National governments recognise the internet domain as a component of their sovereignty

It is worth mentioning that the MFA of Kosovo has elaborated a National Strategy on Digital Diplomacy, which includes such interesting and ambitious projects as App Camp, Wiki Academy, Digital Kosovo Initiative, Kosovo Diaspora Agency, and #InstaKosovo (its diplomats around the world are engaged in propagating the young republic as the New Europe). Kosovo's political leadership also succeeded in being added to the Microsoft list of supported countries and was, so to

2 C. Bjola, *Digital Diplomacy 2.0: Trends and Counter-Trends,* "Revista Mexicana de Política Exterior", 113, 2018, p. 3 [https://revistadigital.sre.gob.mx/images/stories/numeros/n113/bjolai.pdf access: 02 May 2020].

3 S. Riordan, *Cyber Diplomacy vs. Digital Diplomacy: A Terminological Distinction,* University of Southern California, Center on Public Diplomacy, 12 May 2016 [https://www.uscpublicdiplomacy.org/blog/cyber-diplomacy-vs-digital-diplomacy-terminological-distinction access: 07 May 2020].

4 M. J. Randazza, *Kosovo's Digital Independence: Time for Kosovo's ccTLD,* "Wisconsin International Law Journal", 33(4), 2016, p. 670.

say, "recognised" by Facebook. Today, you can find Kosovo on Google Maps. Their digital diplomacy is enforced by YouTube, Flickr, and Google+. In 2017, a Twiplomacy report announced the MFA Kosovo account ranked 31st out of 50 "Best Connected World Leaders" in terms of interconnections with other diplomacies on social media.[5] Thus, it means that gradually ICTs have enabled Kosovo to move beyond the borders of the regional conflict, to be more present in the global processes, and to be perceived by the wider public as a fully sovereign state without the unanimous *de jure* recognition.

> ***relations between states in cyberspace may positively or negatively affect even partnerships established long ago***

The case of such self-proclaimed states as Transnistria, Northern Cyprus, Somaliland, Nagorno-Karabakh, South Ossetia, and Abkhazia is different. Their "independent" status was gained by means of hard power. These state formations succeeded to establish governments and courts; they control their territories and possess the other characteristics of statehood without being recognised. However, they are much less active in the cyber domain. We are not even able to talk about any strategic vision in this respect, which could be a backup means in terms of their international recognition.

A big trend for the *de facto* states is to create websites from which they espouse the virtue of their territories. They claim two things: that they already function as stable, effective entities and that they are democratic. They seek to attract foreign investment and tourists but admit that it is extremely hard to do so. Skype and Amazon do not include these territories, and they do not feature on Google Maps or similar sources. And definitely the online progress is prevented by the absence of ccTLD. For this reason, Nagorno-Karabakh usually borrows Armenia's domain, Somaliland uses .com, and Transnistria – .org.[6]

One more interesting example is Estonia, a small Baltic state that has succeeded in making the digitalisation of public life a part of its soft power, a driving force of public diplomacy, and today sets trends in the cyber realm. Estonia became the first country in the world to open a Data Embassy in another country. In 2018, the Estonian Parliament passed an act that allowed it to host critical databases in Luxembourg. This is not an embassy in the traditional diplomatic sense, and while the founding agreement does take into account the Vienna Convention on Diplomatic Relations, it is something completely new under international law. It is fully under the control of Estonia but has the same rights as physical embassies, such as immunity.[7] Certainly, it is a breakthrough in cyber diplomacy.

Yet another signal of interest resides in the merging of the state and private sectors in cybersphere. For instance, Data Embassy is

5 A. Visvizi, D. L. Miltiadis (eds.), *Politics and Technology in the Post-Truth Era,* Emerald Publishing Limited: Bingley 2019, p. 200.

6 N. Caspersen, *The Politics of Getting Online in Countries that Don't Exist,* "The Conversation", 14 January 2014 [https://theconversation.com/the-politics-of-getting-online-in-countries-that-dont-exist-21399 access: 11 May 2014].

7 *Data Embassy*, e-Estonia Briefing Centre, n.d. [https://e-estonia.com/solutions/e-governance/data-embassy/ access: 08 May 2020].

an extension in the Cloud of the Estonian government, designed in collaboration with such companies as Cybernetica, Dell, EMC, OenNode, Telia, and Ericsson.[8] This is a new tendency with the direct implementation of a multistakeholder approach, which can be adopted worldwide.

From Cyber Diplomacy to Cyber Politics

Today we can spend long hours arguing whether the cyberspace is as virtual as we used to think or has a direct impact on what is happening in real life. In this context, I would suggest considering it as another dimension of reality, and contemporary politics is not an exception. All known forms of political interaction, be it cooperation or conflict, demand from the world leaders to be ready to jump in. Taking into account the growing number of people who have access to the internet and advanced technologies, the cyber domain turns into a critical security issue and should be attributed to high politics.

Cyberspace requires a different level of address in addition to the other three already existing – "human", "states", and "international system", emphasising the separation between the "social system" and the "natural environment".[9] And this new level is characterised by a plethora of interdependent players. It makes diplomacy more vulnerable and fragile. In other words, relations between states in cyberspace may positively or negatively affect even partnerships established long ago. If during the Cold War, the Soviet-American rivalry was predominantly resulting in an arms race, today states possessing technical capabilities compete in cyberspace.

Both strong and weak actors try to control this "battlefield" by various means, whether setting "the rules of the game" or filtering the internet content with the view to defend themselves from malicious actions and even cyberattacks. But it is an outstanding issue: whether cyber threats can or should be perceived as a peril for state sovereignty and what is more – call for a military response.

"it is an outstanding issue: whether cyber threats can or should be perceived as a peril for state sovereignty and what is more – call for a military response

Cybersecurity remains a matter of national security and protection of a country's interests, although governments are gradually moving the debates over safe and stable connectivity infrastructure ever more toward intergovernmental fora and bilateral agreements. Along this line, the UN has formalised a multilateral approach to cybersecurity, specifically through the establishment of the UN Group of Governmental Experts (GGE)[10] in 2004, intended to "advance responsible State behaviour in cyberspace in the context of international security". The group's mandate covers the following topics:

8 Ibid.

9 S. Abedi, *The Priorities of Cyber Diplomacy in the Rouhani's Government,* "Modern Diplomacy", 02 December 2019 [https://moderndiplomacy.eu/2019/12/02/the-priorities-of-cyber-diplomacy-in-the-rouhanis-government/ access: 10 May 2014].

10 A. Calderaro, *Overcoming Fragmentation in Cyber Diplomacy: The Promise of Cyber Capacity Building,* Italian Institute for International Political Studies, 02 April 2020 [https://www.ispionline.it/en/pubblicazione/ overcomingfragm entation-cyber-diplomacy-promise-cyber-capacity-building-25418 access: 04 May 2020].

- Existing and emerging threats;
- How international law applies in the use of ICTs;
- Norms (non-binding), rules and principles of responsible behaviour of States;
- Confidence-building measures;
- Capacity building.[11]

Basically, the GGE works on the elaboration of principles that states should obey in cyberspace, generating recommendations that can stimulate further consultations on their implementation. But one drawback that significantly slows down the process is that the GGE operates on the consensus basis, and if at least one of its members were against, a jointly prepared final report wouldn't be released, which happened in 2017.

Previously, in the *GGE Report 2013,* it was concluded that the international law and the UN Charter should be applicable in cyberspace, but disagreements arose about how to do it. The discussion collapsed when the group could not find common ground over the rights of states to respond to internationally wrongful acts committed through the use of ICTs and the applicability of international humanitarian law in cyberspace.[12] The opposing parties were the United States and the Russian Federation, which were aggravated by the extremely unfavourable geopolitical environment connected with the illegal annexation of Crimea. An additional variable in this already complicated equation became China, which has been the Russian ally in promotion of a *Draft Code of Conduct for Information Security* at the UN since 2011. Thus, the two countries demonstrated a concern that information content itself could represent a threat to national security and set out a series of measures for maintaining sovereign control of their "information space".[13]

Indeed this contradicted the Western approach to "cyber security", but what is notable is that it mirrored the situation in the UN Security Council with the voting on important political issues. Thus, a certain ideological split, fuelled by the primacy of national interests, resulted in the "refashioning" of the GGE format and establishment in 2019 of an Open-Ended Working Group (OEWG). It actually reaffirmed the abovementioned confrontations, but was framed as a forum where any interested UN member state could participate, underlining the inclusiveness of the recently founded entity. Civil society and industry representatives became the new stakeholders in this process, and may definitely contribute to the negotiations around international law and internet governance models.

But what gives a cause for concern is that from now on the work on the future binding norms for cyberspace will be conducted on two parallel tracks and this may dilute the main focus. Under these circumstances, it is very easy to massively politicise the problem, and in such a way that the workflow will simply get stuck with terms and definitions.

The UN still remains a unique international platform for the identification and mitigation of global issues. It is possible to say with

11 *Group of Governmental Experts,* Office for Disarmament Affairs, United Nations, n.d. [https://www.un.org/disarmament/group-of-governme ntal-experts/ access: 12 May 2020].

12 *S. T. Colatin, A Surprising Turn of Events: UN Creates Two Working Groups on Cyberspace, NATO CCD COE Law Branch, n.d.* [https://ccdcoe.org/incyder-articles/a-surprising-turn-of-events-un-creates-two-working-groups-on-cyberspace/ access: 10 May 2020].

13 D. Stauffacher, *UN GGE and UN OEWG: How to Live with Two Concurrent UN Cybersecurity Processes,* "ICT4Peace to Jeju Forum", 30 May 2019 [https://ict4peace.org/publications/un-gge-and-un-oewg-how-to-live-with-two-concurrent-un-cybersecurity-processes/ access: 09 May 2014].

confidence that the world community is far from developing legally binding norms for cyber domain, but every joint effort helps building trust between the actors, raising awareness of the coming threats, and enhancing transparency and predictability among the states. At this point of time, we need a clear road map, which defines the "red lines" in cyberspace, answering the questions of what is allowed and what is not, who is responsible, and what the punishment for a particular cybercrime should be. In this case, the pieces of state practices are highly important.

Publishing of national strategies and action plans, exchange of experience in repulsing cyberattacks domestically will set the precedents that can complement international law. Capacity building is an essential component in this regard. Supporting the establishment of national structures and internal mechanisms on countering cyber threats, sharing the lessons learned on resilience measures, organising specialised courses of study, professional trainings, conferences, and workshops are not only useful for the bridging of digital divides between the parties engaged but also a big investment in their sustainability relevant to cybersecurity.

Security Dilemmas in Cyberspace

There is no doubt that the internet is the most powerful information source, which not only is used for communication or entertainment but also poses certain security risks connected with data protection, human rights violations, and breach of international law. Thus, we observe a shifting of focus from the societal aspect of information dissemination to its protection. The "weaponisation" of data creates a new space for rivalry and warfare, where the interests of states may clash.

When it comes to "offline" or "classical" international conflict, the parties have clear guidelines to follow (treaties, customary law, general principles of law, etc.) or official institutions to appeal to (International Court of Justice, International Criminal Court). But what should be done if a cyber conflict is beyond the threshold of the use of force? Or how is this virtual borderless space – where vital national interests of states are infringed upon and the repercussions are noticeable in the physical world – regulated? This is exactly the discourse in the frame of which the discussion flows. Of course, it does not mean that the absence of a cyber-specific system of international legal rules leaves the cyberspace uncontrolled. As was mentioned before, the UN Charter serves as the basic set of norms, but it does not give a comprehensive answer to all emerging questions.

Let us explore more precisely the Distributed Denial-of-Service (DDoS) attack against Estonia in 2007 and refer to the UN Charter Article 51, which says that states can legitimately use force in self-defence in response to "a significant armed attack" and in proportion to the injury suffered.[14] The first point at issue is whether we can equate an armed attack with a cyber one. Against this background, legal experts advise to turn to the measurement of the material damage that has been caused. In this case, the cyberattacks targeted websites of the Estonian president, government, parliament, and prime minister, political parties, media outlets, and major banks. Some of them were blocked, degraded for days, or slowed down their work. And despite the fact that the functioning of virtual entities was harmed,

14 S. Soesanto, S. F. D'Incau, *The UN GGE Is Dead: Time to Fall Forward,* European Council on Foreign Relations, 15 August 2017 [https://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance access: 03 May 2020].

the disruptive actions came at a high cost, with an estimated economic impact between 27 million and 40 million US dollars.[15] In view of this, we cannot call it an "attack" with non-material effects, but still, was it enough to apply legally binding norms to the perpetrator?

Another matter of concern is Article 5 of the Washington Treaty. In 2007, Estonia had been already enjoying its full membership in NATO. Legal instruments to prove that the abovementioned cyberattack should be treated in the same way as a military one could have enabled the Estonians to trigger Article 5. However, it did not happen, not even because of legal collisions, but most likely due to the unwillingness to start a real-life military conflict when there were no civil casualties and the economy of the victim party was not devastated at large.

To bridge existing legal gaps, an international group of experts under the initiative of the Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence issued the *Tallinn Manual on the International Law Applicable to Cyber Warfare* in 2013, with an expanded 2nd edition – *Tallinn Manual 2.0* – in 2017. The textbooks represent a comprehensive study, covering both the most severe cyber operations and common cyber incidents between states. With regard to the use of force in cyberspace, Rule 11 of the *Tallinn Manual* states: "A cyber operation constitutes a use of force when its scale and effects are comparable to noncyber operations rising to the level of a use of force".[16] In the commentary to the rules, the authors note that generally "[a]cts that injure or kill persons or damage or destroy objects are unambiguously uses of force" and where cyberattacks have similar consequences, they are "highly likely" to constitute use of force.[17] In reality, these statements echo the main principles of the UN Charter named before but, unfortunately, have no legal power and may be used as a theoretical basis for future work in this area.

In terms of the ongoing global discussion on responsible state behaviour and international law in cyberspace, the EU is an active contributor as well. In June 2017, EU ministers of foreign affairs came up with a joint EU diplomatic response to malicious cyber activities under the title *Cyber Diplomacy Toolbox* (CDT). The idea is about the application of sanctions mechanism aiming to develop signalling and reactive capacities at the EU and member state level with the aim to influence the behaviour of potential aggressors, taking into account the necessity and proportionality of the response.[18] Of course, the concept is not new by itself, because the EU has been using it for the past three decades. This kind of restrictive measures may become a universal remedy to "punish" those who do not play by the rules. Here the problem also lies in how to turn sanctions into an effective external action (the EU Common Foreign and Security Policy), implementing them proportionally to the committed crime, and this would certainly require unanimity among member states on the Union's cyber engagement.

---

15 S. Li, *When Does Internet Denial Trigger the Right of Armed Self-Defense?*, "Yale Journal of International Law", 38, 2013, p. 182.

16 M. N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare,* Cambridge University Press: New York 2013, p. 47.

17 S. Haataja, *The 2007 Cyber Attacks against Estonia and International Law on the Use of Force: An Informational Approach,* "Innovation and Technology", 9(2), 2017, p. 166.

18 E. Moret, P. Pawlak, *The EU Cyber Diplomacy Toolbox: Towards a Cyber Sanctions Regime?*, European Union Institute for Security Studies (Brief Issue), July 2017 [https://www.iss.europa.eu/content/eu-cyber-diplomacy-toolbox-towards-cyber-sanctions-regime access: 09 May 2020].

Conclusion

In the twenty-first century, cyber diplomacy will not replace the "old style" practices but will certainly become an inalienable part of them. While enhancing communication and establishing strong linkages between politicians and people, it will further function as an international platform for producing new ideas, social movements, and global trends. This is a moment of transition – an era of rapid change at the intersection of technology and foreign policy, where the work of diplomats is to increase the speed at which governments can respond to that change.[19]

> ***The development of legally binding norms and international law in cyberspace remains a challenge for global leadership***

In this sense, the outbreak of the COVID-19 pandemic gives an additional impetus to these transformations, pushing the whole world into cyberspace. It is certain that nobody could predict online diplomacy becoming the only possible way to interact even for a limited period of time. The value of "personal diplomacy" increased significantly, making reliable partnerships stronger than ever before and accelerating the decision-making process.

It is clear enough that in the post-coronavirus world, the digitalisation of diplomacy will continue, facing all the threats coming from the cyber domain. The protection of critical infrastructure will be a primary task, placing the problem of cyber hygiene on both domestic and international agenda. For this reason, it is urgently needed to keep the dialogue going within the UN GGE and OEWG, despite the substantial differences of opinions.

The development of legally binding norms and international law in cyberspace remains a challenge for global leadership. There is no certainty about their attribution, the conditions under which countermeasures should be taken, and their proportionality. It may be reasonable to use sanctions as a tool to constrain those who seek to compromise international legal principles in virtual reality. But the sanctions mechanism is rather sophisticated and demands a single approach to cybersecurity and digital policy. Due to this, it is necessary to intensify the collective efforts of the like-minded partners (not only states but non-governmental actors as well) in order to share their experiences regarding the use of cyberspace. Only by expanding their cyber capacity building can the diplomatic channels of communication via the internet be safer and more reliable.

Olga Rusova, *PhD in Political Science, is a Chief Specialist at Odesa Regional Office of the Hennadii Udovenko Diplomatic Academy of Ukraine. In the 2019/2020 academic year, she took part in a nine-month post-graduate diploma programme in the theory and practice of International Relations and European Integration at the Estonian School of Diplomacy. Olga is the author of 12 scientific articles and contributed to one collective monograph; she has been a participant of more than 20 Ukrainian and international workshops and trainings. Her research interests are the foreign policy of Germany and Poland, issues related to the course of European integration process, and the EU security policy.*

19 *21st Century Statecraft*, "Diplomacy in Action", the US Department of State, 20 January 2017 [https://2009-2017.state.gov/state craft/overview/index.htm access: 02 May 2020].

Issue 2 (20), 2020
ISSN 2518-7481