# CYBER DIPLOMACY 3.0 - "AGILE DIPLOMACY" TO PROMOTE SECURITY AND INNOVATION

**Amit ASHKENAZI**
Adjunct Lecturer
Haifa Center for Law and Technology, Faculty of Law, University of Haifa
ashkenazia@tauex.ac.il

**Abstract:** This article discusses developments in Western domestic and international Information and Communication Technology (ICT) policy and their implications for the practice of diplomacy, or "cyber diplomacy". The article describes three phases of domestic and international cyber policy. The first period was characterized by a Western "hands-off" approach, in order to promote free flow of information and innovation. The rising importance of ICT to national security and state interests, civic awareness to privacy on the internet, as well as concerns regarding various ICT market failures, caused a policy shift. Cyber policy and diplomacy 2.0 is an era in which discussions about applying and developing the international rules-based order for the cyber domain was prominent. This called diplomacy to center stage, to deal with geopolitical, technical and social complexities of this field. While some progress was achieved, geopolitical tensions have caused these efforts to be insufficient to promote security and stability on the internet. Meanwhile, domestic policy making activity relating to ICT has had cross-border effects, which have also caused frictions to the ICT ecosystem. This has led to "Cyber policy 3.0", a policy focused on developing better coordination and cooperation between like-minded states to promote ICT resilience. In order to fulfill the promise of Cyber policy 3.0, cyber diplomacy needs to develop robust interfaces with domestic policy processes and advanced toolsets.
**Keywords:** Cyber policy, Cyber Diplomacy, ICT, internet governance, multistakeholder, cross-border cooperation, agile regulation, innovation.

## INTRODUCTION - POLICY AND DIPLOMACY IN A GLOBAL ECONOMY

In this contribution I would like to describe the current challenges and opportunities for effective diplomacy in the field of Information and Communication Technology (ICT).

Diplomacy is the conduct of relationships, using peaceful means, by and among international actors, at least one of whom is governmental. It is the discipline through which foreign policy is practiced. (Cooper et al., 2013, p. 2) While diplomacy has existed as part of governance and international state to state relations since antiquity, it faces challenges that reflect the complexity of policy and the international arena in a global world. (Cooper et al., 2013, p. 21). In general, diplomacy in the 21st century is highly connected to domestic policy making and political and societal demands about governance in a wide variety of issues (Cooper et al. 2013, p.1). Policy is effected by policymakers' need to balance among the different interests and actors, between domestic demands and international imperatives, between the national constituency and the international community, between principles and pragmatism, and between the immediate, medium, and long terms (Cooper et al. p. 15). These challenges are especially relevant to the ICT ecosystem because of the dominance of the private sector in it, the quick pace of developments, and its global nature.

These two challenges, development of domestic and foreign policy, and executing it, are highlighted in many areas of modern governance, that like ICT, are both technical and global in nature, such as tax, financial regulation, environmental regulation.

In order to explore these challenges in the ICT context, the contribution surveys the development of "cyber" policy and diplomacy, and argues that it can be divided into three phases, with expanding roles for diplomacy.

The first period, "Cyber policy and diplomacy 1.0", was characterized by a Western "hands-off" approach policy to ICT, in order to promote free flow of information and investment. The second period, Cyber policy and diplomacy 2.0 is an era in which discussions about developing international rules to deter malicious activities were prominent, due to rising cyber risk. The UN and many other international venues discussed the application of international law to ICT and developing norms of responsible state behavior in order to promote stability and security. Even though there was much international activity, its impact on security and stability can be questioned. The third period is Cyber policy 3.0, which is symbolized by " A Declaration for the Future of the Internet", launched in 2022 by the United Stated and 60 states (U.S. Department of State, 2022). Cyber policy 3.0 shifts from developing norms against malicious activities, to better coordination and cooperation between likeminded states to enhance resilience. Each of these policy periods sets different goals for cyber diplomacy, and has lessons for making diplomacy more effective given the complex institutional arena. Following the description of these phases, some reflections on effective "cyber" diplomacy will be offered.

## CYBER POLICY 1.0

The development of the internet from an academic research project to a market led commercial space created a new "technical-social phenomenon" made by man. Law and policy developed gradually by adapting existing legal rules to the ICT context. While there were early attempts to set rules for the internet they were faced with legal policy and technical challenges, that in a general manner led to a hands-off approach. It was seen as promoting innovation, speech, human rights and democratic values to let the internet develop without the state developing new laws and regulations.

This policy reflects a careful approach that does not interfere in markets without information, and relies on self-regulation by the market to deal with unwanted phenomena. It aims to prevent frictions that may stifle innovation and the free flow of information and investment. One leading example, is a unique liability regime developed in the United States for internet intermediaries. It is highly influential because it exempts internet intermediaries (such as search engines and social networks) from liability for content produced by their users, that they distribute. It reduces potential legal restraints that intermediaries may place on distribution of user content, and therefore it is considered to be one of the core legal contributions to innovation on the internet (Goldman, 2017; Samuelson, 2020).

This general careful approach can also be explained as a result of the gap between policy, technology and markets. Companies constantly develop new services and products, and

keeping up with them raises challenges for developing and deploying public policy. Challenges for public policy stem both from the need to apply society's values and principles to a new situation, and from the risk of new rules having "unintended consequences" or chilling effects on innovation. One approach to possible policy development that aims to deal with these challenges was promoted by The US National Telecommunications and Information Administration. This policy puts an emphasis on a "multi stakeholder" approach to deal with developing policy responses to new technologies. In these processes government does not regulate "top down" but rather convenes all of the relevant actors from the industry and civil society. As explained by Strickling and Hill, these processes have advantages when compared to more traditional regulatory and legislative models. This is because the traditional approaches are lengthy and formal. Thus they can not keep pace with developments. One such example is the way internet standards are developed (Strickling & Hill, 2018, p. 47). The criticism against these processes is that they may lack effective enforcement mechanisms, and therefore rely on their voluntary adoption by the different players.

## FROM DOMESTIC POLICY TO INTERNATIONAL ENGAGEMENT – CYBER DIPLOMACY 1.0

In the first era of cyber diplomacy, western diplomacy echoed these domestic policy goals on the global stage. The basic western approach to the issues of "governance" was that in this area, a multistakeholder governance model was needed. As a result, internet governance spans many "governors" which include not only the national governments, but also many types of "non state actors", including technology corporations and other private sector players. (De Nardis, 2020, p. 3).

This immediately calls attention to the potential challenges for the diplomatic trade. This policy by definition requires diplomats, versed in the state to state arena, to interact in the global arena with so called "non state" actors. If aiming for what Strickling and Hill call an "authentic" multi-stakeholder model (Strickling & Hill, 2018, p. 49), without even a special position or power for government around the table. In other words diplomacy is required to be practiced in an open arena, which does not include only diplomats, and without a special advantage to state actors.

Yet this challenge did not materialize at that time, because the policy goals in the international arena were relatively straightforward. The discussion was focused on the way internet domain names should be managed globally. The Western position was to rely on the existing multistakeholder frameworks that relied on the activity of the American Internet Corporation for Assigned Names and Numbers (ICANN). This was not the position of other countries, where the view was that the internet and ICT need to be governed as any other aspect of social and economic life, within the remit of the state.

Thus, the discussion in the state to state arena was focused on the preliminary question of dealing with this issue in an international organization, or not. Indeed, the diverging views were heavily connected to different views as to the role of the state in regulating content on the internet. While Western approaches are careful with state intervention in production and

distribution of content due to the importance of freedom of speech in democratic societies, other states see content control as part of their governance authority.

As a result while internet governance is a complex policy area, the actual question on the negotiating table was simple – governance in ICANN or in the dedicated UN telecommunication agency, International Telecommunication Union.

A more realistic approach might argue that these were not the only reasons, and that given the challenges of developing domestic policy for ICT, many states did not have defined preferences or a clear definition of their engagement goals. Given the complex political, economic and technical environment, it is equally reasonable that states have more limited maneuvering possibilities to begin with, which also affect their motivation to be proactive in this area.

This has led to international discussions mainly dealing with the terms of engagement, with less activity regarding the rules on the internet.

One notable exception is the Convention on Cybercrime of the Council of Europe, which created a sophisticated legal instrument to promote cross-border law enforcement cooperation (Council of Europe, 2004). The convention which was developed uniquely between the USA and the Council of Europe, has been ratified by 66 states (Council of Europe, 2022). The COE is an early example of how international cooperative policy, and collaboration between diplomats and subject matter experts have led to an intricate framework, that supports cross border law enforcement activities.

The symbol of this era in the internet governance discussion is the World Summit on Internet Society process, convened by the International Telecommunications Union (The World Summit on the Information Society, 2015a), which officially put the issue of internet governance on the diplomatic agenda (Kurbalija, 2016, p. 7). The differences regarding the role of states in "internet governance" led to a conflict in the meaning of the term "governance" (Kurbalija, 2016, p. 6). The agreed upon definition in the WSIS context, **included** the activities of non-state actors within the term "governance". The World Summit on Information Society definition was: "Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, and programmes that shape the evolution and use of the internet (The World Summit on the Information Society, 2015b). While the WSIS process recognized the rising role of the internet as part of social life and economic activity, it also relied heavily on a multistakeholder view of internet governance. It initiated the "Internet Governance Forum" which has convened since then to discuss various cutting-edge issues of ICT and governance in an open and multistakeholder fashion. While it has been described as the main venue for dialogue about internet governance processes in an open and inclusive manner (Marzouki & Calderaro, 2022, p. 6) from the early days, questions regarding its tangible results were raised, mentioning that "however, some critics claimed that the IGF was only a talk show without any tangible results in the form of a final document or plan of action" (Kurbalija, 2016, p. 7).

During the development of the international multistakeholder discussions in the IGF, many issues related to internet policy in the wide sense came to be discussed. But an attempt to institutionalize more formally these discussions during the 2012 World Conference on International Communications ended in a stalemate (Kurbalija, 2016, p. 11). The main conflict was a non-binding resolution on the role of the ITU in internet governance, that divided participating states into two blocks: Western countries in favour of the existing multistakeholder model, and supporters of the resolution including China, Russia and other countries that preferred an intergovernmental model (Kurbalija, 2016, p. 11).

## DEVELOPMENTS IN DOMESTIC POLICY

As the internet economy developed exponentially, creating new uses, markets and effects on society, domestic policymakers began seeing some of the challenges of the "hands-off" approach, and public opinion and civil society called for policy interventions.

The "data economy" in which personal information was collected on a massive scale, raised concerns about the protection of privacy. The market power of the large ICT companies raised concerns about concentration of market and political powers. The unique limitation of liability regime for intermediaries, allowed these intermediaries to decide what content can be distributed, and questions were raised as to their motivations and discretion. This started a quest for renewed policy measures.

In 2013 the information leaked by Edward Snowden, a former US National Security Agency contractor, caused a major rift in the Western approach as it raised concerns regarding the possible uses of the internet for national security purposes, which were arguably not aligned with the "multistakeholder" free and open internet narrative. The information leaked also led to a trust crisis within the Western states, that required diplomatic mending. In a move that can not be completely disconnected, the US government, began a long and meticulous process to change the ICANN governance model. It shifted from being managed through a contract with the US NTIA, to a stewardship by the global internet community (Kurbalija, 2016, p. 14).

The information leaked not only caused changes in the international internet governance discussion, but had wider effects on the intersection between law and the global internet. It affected one of the key legal and international mechanisms that support the free flow of information across borders, the US-EU "Safe Harbor" agreement. This agreement aimed to enable cross border personal data flows, between the EU and the US, while protecting EU citizens' privacy, even though the US has a very different privacy regime. The "Safe Harbor" agreement aimed to deal with these differences in a way which leads to substantial protection of privacy, taking into account different privacy regimes.

After the Snowden revelations, a concerned privacy activist, Max Schrems, claimed that the "Safe Harbor" is not satisfactory. Mr. Schrems argued that the Snowden revelations about potential US government collection and use of data about EU citizens, requires additional safeguards to protect EU citizens' data that is transferred to the US. The European Court of

Justice accepted the argument, and ruled that the "Safe Harbor" agreement needs revision. The implications of the Schrems judgement were far reaching, in its effects on the data transfers with immediate implications on the trade relationship and the commercial level. (Kuner, 2017).

From an international point of view, this is a unique development of international relations and ICT. The ECJ, a constitutional court of one important jurisdiction applied its legal framework to another important jurisdiction's domestic security practices, with immediate implications on the trade relationship and the commercial level (Atik & Groussot, 2021). Thus, a seemingly domestic ruling has immediate implications for international relations and trade. The US and the EU commission amended the "safe harbor" arrangements to take into account the ECJ guidance, and introduced "Safe Harbor", a more robust agreement. Mr. Schrems appealed again, and the court canceled the new arrangement as well, because it lacked redress mechanisms for EU citizens (InfoCuria Case-law, 2020). These developments brought to center stage not only rules that apply to ICT (data protection regimes), but their effect on global trade relations, and the intersection between security and trade.

The spread of the ICT to many fields of life also ushered the age of "cybersecurity", meaning risks to national security and important state interests from the digital domain (Organization for Economic Co-operation and Development, 2015; European Commission, 2022). This required countries to deal directly with their role in protecting the national cyber domain, as they do with the physical cyber domain. This period called for a more active role on behalf of the government to promote its basic roles, namely providing security and public safety in the online environment.

## CYBER POLICY 2.0 AND IMPLICATIONS FOR CYBER DIPLOMACY 2.0

The rising importance of the internet for core societal functions, coupled with rising risk from cyber operations, led to two challenges for cyber diplomacy: exploring the role of the international rules-based order regarding "cyber operations", and dealing with the increased activity of domestic policymakers and this activity's implications on cross-border relations.

## DEVELOPING RULES OF THE ROAD FOR CYBER OPERATIONS

The rising attention to the risk for important national interests and functions, and the concerns regarding negative effects of cyber operations on national interests, called attention to the role of the international rules-based order in this area. (Schmitt 2020a, p. 33-34)

This called cyber diplomacy to center stage at the UN, to discuss these issues and develop views and understandings about them. While the potential misuse of ICTs and the risks they pose to States and international peace and security were brought to the UN table since 1998 (United Nations Office for Disarmament Affairs, 2022), it seems that actual outcomes were achieved through the Group of Governmental Experts (GGE) Reports, from 2013 (U.N. Secretary-General, 2013) and 2015 (U.N. Secretary-General, 2015).

These negotiations discussed the application of international law concepts to cyberspace, and explored the creation of new norms of responsible state behavior. These interpretations

and rules were based on an effort to use international law and norms to restrain and deter malicious illegal cyber activities. In addition, these efforts included promoting "confidence building measures" and "capacity building". (U.N. Secretary-General, 2015)

These reports reached agreement regarding the applicability of international law, and in particular the UN Charter to the cybersphere. The reports continued in proposing some elements of the way the rules and principles of international law can apply to ICT. In addition, the 2015 report included a list of voluntary non-binding norms of responsible state behavior. These developments aimed to propose how the existing international rule-based order can develop rules for ICT, and effect malicious activity (NATO Cooperative Cyber Defence Centre of Excellence, 2015).

The 2015 GGE report seems to be the highlight of this era in the more traditional diplomatic activity. Yet, developing these rules that apply to cyber operations has proven to be a challenging task due to the unique features of cyberspace. (Schmitt 2020a, p. 16). A strong position has been put forward as to the "extra layer of caution in determining how exactly international legal rules apply to cyber operations, and in evaluating whether and how additional rules should be developed" (Schondorf, 2020b; Schmitt, 2020). These are doctrinal issues with the development of international law for cyber operations, that emphasize the difficulty of creating new cyber norms.

Yet in the international arena, the political tensions have a major role as well. The failure of the following Governmental Group of Experts that convened in 2017 to reach consensus, brought the political tensions to the forefront (Schmitt & Vihul, 2017). They caused one of the officials involved to reflect that: "I am coming to the unfortunate conclusion that those who are unwilling to affirm the applicability of these international legal rules and principles believe their States are free to act in or through cyberspace to achieve their political ends with no limits or constraints on their actions." (Schmitt & Vihul, 2017). Maurer reflects that the collapse of the 2017 GGE marks a break in the international discussion on cyber norms. He describes the collapse of the process as due to a combination of geopolitical tensions, competing tactics, and growing pressure to open the process to others. (Maurer 2020, p. 298).

Maurer highlights the collapse of the 2017 UN GGE against the backdrop of two of the more influential global cyber events, "notPetya" and "Wannacry". Both of these cyber events involved massive disruption and damage. Maurer comments that the geopolitical tensions and heightened security concerns overcame the need to cooperate to deal with the deteriorating security environment. (Maurer 2020, p. 298). One of Maurer's conclusions is that the "top-down" diplomatic negotiations represent only one piece of the puzzle". (Maurer 2020, p. 300).

## DEVELOPMENTS IN OTHER INTERNATIONAL VENUES

In 2014, Prof. Nye discussed the "The Regime Complex for Managing Global Cyber Activities" and offered a schematic map of "cyber governance" activities that highlights the

diversity of "norms, institutions and procedures" in this area (Nye, 2014). Finnemore and Hollis also stress the importance of the normative context in which norms are developed, and the fact that there are many norm communities. (Finnemore & Hollis, 2016)

In addition, the rising activity of domestic policymakers, while tailored according to different societies' approaches, has had de facto cross-border effects as the Schrems case shows. Some measures are directly intended for cross-border effects (such as the rules on exporting data under the EU General Data Protection Regulation), while others may reach this result unintentionally. Thus these domestic measures affect the legal environment that applies to international business, and can have more effects in the international sphere than the formal international discussions. (Bradford, 2021). They can also effect the ability to cooperate not only in commercial matters, but also in resilience related cooperation, such as sharing information about malicious cyber actors and their techniques. (Swire & Kennedy-Mayo, 2022).

During this period, cyber diplomacy evolved from the more "hands-off" approach of the WSIS process, to adapt to protect national interests, and promote them in the international arena. As states began to investigate a more active approach in this area, they needed to discern the complexity of multiple arenas in which ICT related activities are developed on the global field.

These two major trends required cyber diplomats to build bridges, yet while the domestic policy that guides the *architecture* of the bridges was still under development.

## TRANSITION IN CYBER POLICY AND DIPLOMACY?

In the meantime, a new paradigm emerged, that of enhancing cooperation between like-minded states, to achieve resilience. The first major sign of this trend was the Prague 5G conference (Government of the Czech Republic, 2019) which brought together like-minded states to discuss how to protect this next generation technology.

This conference brought to the table a more focused diplomatic vision for the security and stability of the internet – promoting trust and interoperability between likeminded states. Instead of focusing only on the malicious actors (and given the arguable lack of effective legal tools and geopolitical tensions), this avenue promotes resilience in the civilian infrastructure, so that it is less susceptible to cyber-attacks and misuse.

The Prague process required the diplomatic craft to involve both negotiation skills, national, regional (EU) and international interests, and a technical and economic understanding of the telecom ecosystem. The Prague process itself brought together several workgroups, in which diplomats and policy experts worked together.

In the 2019 IGF the application of this concept to cybersecurity was also discussed at a specific session, to promote bottom-up cooperation on cybersecurity, by reducing legal barriers to cross-border cooperation (The Internet Governance Forum, 2019).

These two examples, one a full-fledged conference and the other an IGF open forum share the motivation to promote security and stability on the internet, but do so not by focusing on

more rules against malicious actors, but rather by promoting resilience through cooperation between those that want to cooperate.

This trend relaxes some of the complexities in this area because it is based on a shared will to cooperate, and therefore arguably does not require an enforcement mechanism (Benvenisti, 2020). As seen above, the failure of the 2017 GGE because of tensions happened despite the need to cooperate for a secure internet. Recently, the World Economic Forum warned of the growing cyber risk and the need for better coordination across jurisdictions. (World Economic Forum 2022, p. 49).

From a private sector point of view, there are growing cross-border tensions that risk the fragmentation of the internet, and ultimately the safety and security of the internet. It is important to clarify that this observation does not look at the "chilling effects" of regulation on technology in a domestic setting but rather focuses on the cross-border effects of different domestic regulatory regimes in this area. One of the leading examples is the ability to use cross border ICT cloud services. Cloud services enable scalability and efficiency in processing and storage, but some of the cross border legal tensions cause friction to their use.

In the 2019 IGF the Internet and Jurisdiction Policy Network presented a study that surveyed 150 key stakeholders from the Internet & Jurisdiction Policy network that had the following results: "95% see cross-border legal challenges on the internet becoming increasingly acute in the next three years; Only 15% believe we have the right institutions to address these challenges; and 79% consider that there is insufficient international coordination". The report warns of a dangerous trend in which public and private policy initiatives are uncoordinated and this will have detrimental consequences. The report calls for innovative coordination and cooperation mechanisms to make sure that the fundamental attributes of the internet are preserved (Internet & Jurisdiction Policy Network, 2019, p. 14).

Thus, two trends can be observed. One focuses on better collaboration between like minded states. It builds on the strong link between resilience of the ICT sector, innovation and economic resilience in general. The other trend is more activity on the part of domestic policymakers, that can effect the viability of economic cooperation. Given the geopolitical and economic developments, these growing tensions can conflict with the approach promoted by the Prague 5G conference – creating resilience through the markets. Indeed, reducing unnecessary friction in cross border flows of technology, investments and information, that enable better cooperation facilitate a secure and safe internet. Therefore while developing domestic policy to protect public interests, their effects on global cooperation should be noted.

## CYBER POLICY 3.0

The Declaration for the Future of the Internet (U.S. Department of State, 2022) is a key moment in recognizing the role of the state (and diplomacy) for rules that apply to the internet. The declaration has geopolitical motivations (Kerry, 2022), and its content reflects the change in policy approaches to ICT.

This declaration, led by the United States and supported by many countries, acknowledged both the importance of the internet for society and humans, but also recognized the role of active public policy and the state in promoting the public interest on the internet. Thus, this statement calls for active government interventions with public policy tools, to protect the freedom of the internet. The declaration includes principles for policy activity in this area. It promises that: "Partners in this declaration intend to work toward an environment that reinforces our democratic systems and promoted active participation of every citizen in democratic processes, secures and protects individuals privacy, maintains secure and reliable connectivity, resists efforts to splinter the global internet, and promotes a free and competitive global economy". (U.S Department of State, 2022.)

Thus the declaration sets active policy goals for states, which is different than the original "hands off" approach. Given the global nature of ICT, the declaration also leads to the need for policy coordination, to minimize unnecessary frictions.

A concrete example of negotiations that are part of such policy coordination and reducing barriers, are the developments in the field of cross border data transfers. Following the ECJ ruling in the second ECJ Schrems case, that disrupted US-EU data transfer mechanisms, the US and EU have revealed a new arrangement. Interestingly enough, the US statement includes a commitment by the United States "to implement new safeguards to ensure that signals intelligence activities are necessary and proportionate in the pursuit of defined national security objectives, which will ensure the privacy of EU personal data and to create a new mechanism for EU individuals to seek redress if they believe they are unlawfully targeted by signals intelligence activities" (The White House, 2022). This statement is unique because while the US has a robust system of oversight over their signals intelligence activities (Swire, 2016), this framework does not include the "necessary and proportionate" test, which is part of EU (and not US) constitutional law. Nevertheless, the statement explains that this is so because: "it reflects the strength of the enduring U.S.-EU relationship, as we continue to deepen our partnership based on our shared democratic values" (The White House, 2022).

The more general roadmap to develop cross border ICT cooperation can be seen in the US-EU Trade and Technology Council (U.S.-E.U. Trade and Technology Council, 2021). This process focuses on dealing with cross-border coordination challenges, as part of building ICT robustness and resilience. While it is a bilateral agreement between the EU and the US, it sets policy directions and promotes a clear and strong agenda.

Section 5 of the statement from May 16 2022 reflects this policy and diplomacy vector: "We confirm that we will continue to oppose actors who threaten the multilateral rules-based order and fundamental principles of international law. To protect our citizens, we will draw upon our bilateral trade and investment relations, our joint technology leadership, the transatlantic security partnership, and our shared democratic values. Our cooperation and coordination on the TTC are essential to this effort and we are committed to maintaining the TTC as a central pillar of our transatlantic partnership."

The statement follows on to draw a diplomatic roadmap to promote this cooperation (including at the World Trade Organization). It also includes a list of evolving ICT policy issues which can benefit from better coordination and cooperation, such as 5G and 6G, Artificial Intelligence, quantum computing, supply chain, and foreign investment screening.

The TTC statement illustrates the pragmatic policy direction for Cyber Policy 3.0, and it requires Cyber Diplomacy 3.0 to focus on coordination and cooperation between likeminded states by dealing with potential policy conflicts, and mitigating them.

It highlights the importance of cooperation between like minded states to deal with differing approaches to ICT (such as data protection rules), in order to promote innovation and cross-border collaboration. Reducing unnecessary friction in cross-border flows of technology, investments and information, facilitates a secure and safe ICT environment that is based on the rule of law, democratic values and human rights and promotes innovation and prosperity.

## FROM POLICY TO DIPLOMACY – BUILDING CYBER DIPLOMACY 3.0

The more active role for domestic policy in the field of ICT, and the need to reduce the cross border frictions, require engaged diplomacy. As described in the Oxford Handbook on Diplomacy "It is a critical instrument in an age of complex interdependence and of globalization." (Cooper et. Al, 2013, p.1). Yet the growing challenges (and opportunities) to promoting global security and inclusiveness call for revisiting the necessary diplomatic toolset for the cyber diplomacy, and the complementary interfaces with its domestic ICT policy counterparts.

The current state of play in diplomacy is complex. Even before adding the geopolitical social and economic elements of ICT policy, Mills has written: "In sum, to reiterate, sovereign states no longer control international relations. The expansion in the number of actors has two major implications: First, this greatly complicates the management of foreign policy, where more is expected of a foreign service (often with diminished capacity and resources) in an age where there is greater external and domestic scrutiny and interaction. The concept of international relations no longer means the same as traditional diplomacy, epitomized by 'intergovernmental' or 'interstate' relations, and has implications for the type and quality of personnel recruited and trained for a foreign service. Second it presents enormous new opportunities." (Mills 2013, p. 406).

It seems that the first emphasis for the development of "cyber diplomacy" is not unique to "cyber" but is a general requirement for modern diplomacy. As described in the Oxford handbook on diplomacy, is that diplomacy needs to move from the "club" model, that has developed in a traditional manner, in which diplomats talk with other diplomats to "network diplomacy".

The "club diplomacy" model leads to a "severe disconnect between diplomats in many parts of the world and the realities that they are faced with". The "club model" is important but needs to take into account other actors and groups (Cooper et al., 2013, p. 23). This also

requires better intragovernmental coordination to conduct efficient foreign policy (Mills, 2013). While the club model may have been effective at the GGE process, where the focus was state activity only, the new arena requires adaptation.

I would like to focus on additional elements that include more digital and domestic policy literacy, effective interfaces with domestic officials, and learning from domestic advanced ICT governance techniques.

Digital literacy is important to enable the cyber diplomat to better understand both the goals and the tools in order to reach agreement in this area. Thus, given the focus on developing cross-border understandings on technical-social issues require diplomats for technological and policy literacy. This requires following technical, social, and market development aspects of the internet (Marzouki & Calderaro, 2022, p. 3).

Better domestic and diplomatic interfaces are needed because of the quick pace of changes. In this area even more than other areas, the domestic policy discussion, which includes many players in many forms, such as the media, parliaments and academia, also needs to be accounted for. It seems that it would be useful to draw the cyber diplomat closer to domestic policy negotiations that have cross-border implications.

Bringing the diplomat closer to his policy counterpart, in the field of ICT, can mean also adapting some of the new regulatory approaches to ICT. An important development in domestic regulation and governance of ICT, is "Agile regulation". (Organisation for Economic Co-operation and Development, 2021). "Agile regulation" is aimed to promote regulation focusing on solving market failures while minimizing chilling effects of regulatory intervention. The toolset of "agile regulation" is geared to deal with the challenges of promoting public policy in a fast paced, market led economy, while reducing regulatory burdens. "Agile regulation" includes constant flows of information and expertise between the private and public sector, shorter policy lifecycles, continuous reviews, and institutionalizing multistakeholder governance mechanisms. These tools, seem to resonate with some of the concepts developed in internet governance multistakeholder approach. Indeed, due to domestic policy restraints, they did not fulfill their full potential. But now that policy is on the rise, as depicted for instance by the Declaration for the Future of the Internet, this model can be revisited and applied in other areas. In addition, it addresses one of the major challenges of the global ICT discussion, and that is the role of the private sector and technology companies. These actors are active on the domestic policy front, but also on the global level. Developing a harmonized approach for engagement with them on the domestic and international level, can promote the effectiveness of diplomacy in this area.

Thus, diplomats and domestic policy professionals can benefit from a shared understanding of this meta-language of regulation and governance of innovation, on the domestic-international continuum. Both communities can benefit from tools and techniques such as adaptive iterative and flexible regulatory assessment cycles and improvement of the domestic cooperation. Having a shared view of the challenges and policy reactions will enable them to build upon

their respective training and qualifications to develop and describe to international counterparts their regulatory measures.

## CYBER DIPLOMACY 3.0 – OPPORTUNITIES – IMPROVING CROSS-BORDER COORDINATION

Cyber diplomacy needs to accommodate the goals of Cyber policy 3.0 by improving interoperability between different domestic ICT governance systems.

Developing cross-border understandings on comparative regulatory measures can enable better harmonization, reducing the frictions and promoting interoperability between systems. Because the focus is on solving coordination problems (Benvenisti, 2020) instead of cooperation problems, through promoting a "bottom up" shared view on more technical policy governance objectives and measures, there are more opportunities for agreement.

Creating shared taxonomies, metrics, technical standards and best practices in the regulation of governance of technology can promote policy and legal interoperability.

Sharing regulatory tools and knowledge can help less developed countries deal with emerging technologies (Andia & Chorev, 2017). Given the differences in government-market approaches between "developed" and "developing" nations (Mills, 2013, p. 404), it can support bridging these gaps. This is especially relevant in ICT because of the known timeframes of developing and deploying domestic policy, which lag behind technical-social developments. Thus cross border cooperation can enable developing countries to prioritize their domestic efforts, and perhaps even create innovative policy initiatives that give them a competitive edge. On a more aspirational note, and given the international context, these activities can also generate trust between states by ensuring clarity and enabling seeing similarities and differences in policy measures. (Finnemore & Hollis, 2016, p. 472). Given the challenges of modern diplomacy and the value of cooperation, this can lead to "soft power", that can improve the impact and effectiveness of diplomacy and enable, together with traditional tools "smart power". "Soft Power" is used by Prof Nye to describe effects obtained through cooperation, and "smart power" is a combination of hard (coercive) power and soft power. (Nye 2013, p. 564). It can also support the promise of the Declaration on the Future of the Internet, in the wider geopolitical context.

## CONCLUSION

The rising role of ICT in modern society and its cross-border nature in a global economy require state activity to promote security, trust and stability. In the cross-border context, this can benefit from unique expertise and diplomatic toolset. In order to be effective, and given the shift to promote better coordination in ICT governance, cyber diplomacy should adapt to the challenges, by applying a more interdisciplinary and networked approach, both domestically and internationally.

## REFERENCE LIST


Andia, T. & Chorev, N. (2017). Making knowledge legitimate: transnational advocacy networks' campaigns against tobacco, infant formula and pharmaceuticals. *Global Networks, 17*(2), 255-280.

Atik, J. & Groussot, X. (2021). A Weaponized Court of Justice in Schrems II. *Nordic Journal of European Law Issue, 4*(2), (pp. 21). Los Angeles Legal Studies Research Paper No. 2021-37. Loyola Law School. Retrieved from https://ssrn.com/abstract=3998079.

Benvenisti, E. (2020). The WHO – Destined to Fail?: Political Cooperation and the COVID-19 Pandemic. *American Journal of International Law, 114*(4), 588-597. DOI: 10.1017/ajil.2020.66

Bradford, A. (2021), The Brussels Effect: How the European Union Rules the World, Oxford University Press.

Cooper, A. F., Heine, J. & Thakur, R. (2013). Introduction: The Challenges of 21st Century Diplomacy. In A. F., Cooper, J., Heine & R., Thakur (Eds.). *The Oxford Handbook of Modern Diplomacy*. University Press.

Council of Europe (2004). *Details of Treaty No.185. Convention on Cybercrime (ETS No. 185)*. Retrieved from https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.

Council of Europe (2022). *Chart of signatures and ratifications of Treaty 185. Convention on Cybercrime (ETS No. 185)*. Retrieved from https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185.

DeNardis L. (2020). Introduction: Internet Governance as an Object of Research Inquiry. In: DeNardis L., Cogburn D., Levinson N.S. (ed.) Researching Internet Governance Methods, Frameworks, Futures, The MIT Press, 2020.

European Commission (2022). *NIS Directive*. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/nis-directive.

Finnemore, M. & Hollis, D. B. (2016), Constructing Norms for Global Cybersecurity *110 American Journal of International Law*, *Temple University Legal Studies Research Paper No. 2016-52*, Retrieved from: https://ssrn.com/abstract=2843913

Goldman, E. (2017). The Ten Most Important Section 230 Rulings. *Tulane Journal of Technology & Intellectual Property, 20* (pp. 10). Legal Studies Research Paper. Santa Clara University. Retrieved from https://ssrn.com/abstract=3025943.

Government of the Czech Republic (2019). *Prague 5G Security Conference announced series of recommendations: The Prague Proposals*. Retrieved from https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/.

InfoCuria Case-law (2020). *C-311/18 - Facebook Ireland and Schrems*. Retrieved from https://curia.europa.eu/juris/liste.jsf?num=C-311/18.

Internet & Jurisdiction Policy Network (2019). *I&J Global Status Report 2019*. Retrieved from https://www.internetjurisdiction.net/news/release-of-worlds-first-internet-jurisdiction-global-status-report.

Internet Governance Forum (2019). *Information Sharing 2.0: privacy and cybersecurity*. Retrieved from https://www.intgovforum.org/multilingual/content/igf-2019-%E2%80%93-day-4-%E2%80%93-estrel-saal-c-%E2%80%93-of-45-information-sharing-20-privacy-and-cybersecurity.

Kerry, Cameron F. (2022), *Battle lines for the future of the Internet*, retrieved from: https://www.brookings.edu/blog/techtank/2022/05/11/battle-lines-for-the-future-of-the-internet/

Kuner, C. (2017). Reality and Illusion in EU Data Transfer Regulation Post Schrems. *German Law Journal, 18*(4), 881-918. DOI:10.1017/S2071832200022197

Kurbalija, J. (2016). *An Introduction to Internet Governance*. Diplo Foundation.

Marzouki, M. & Calderaro, A. (2022). Global Internet Governance an Uncharted Diplomacy Terrain. In M., Marzouki & A., Calderaro (Eds.). *Internet Diplomacy: Shaping the Global Politics of Cyberspace*. Rowman & Littlefield Publishers.

Maurer, T. A Dose of Realism: The Contestation and Politics of Cyber Norms. *Hague Journal on the Rule of Law*, *12*, 283–305 (2020)

Mills, G. (2013). Trade and Investment Promotion. In A. F., Cooper, J., Heine & R., Thakur (Eds.). *The Oxford Handbook of Modern Diplomacy* (402-421). University Press.

NATO Cooperative Cyber Defence Centre of Excellence (2015). *Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law*. Retrieved from https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/.

Nye, J. S. Jr. (2014). *The Regime Complex for Managing Global Cyber Activities*. The Global Commission on Internet Governance. Chatham House.

Nye J. S. Jr, (2013), *Hard, Soft and Smart Power*, in: Cooper A.F., Heine J., Thakur R. (ed.) The Oxford Handbook of Modern Diplomacy.

Organization for Economic Co-operation and Development (2015). *Digital security risk management.* Retrieved from https://www.oecd.org/sti/ieconomy/digital-security-risk-management.htm.

Organization for Economic Co-operation and Development (2021). *Recommendation of the Council for Agile Regulatory Governance to Harness Innovation.* Retrieved from https://www.oecd.org/mcm/Recommendation-for-Agile-Regulatory-Governance-to-Harness-Innovation.pdf.

Samuelson, P. (2020). *Pushing Back on Stricter Copyright ISP Liability Rules*. Michigan Technology Law Review Forthcoming Available at SSRN: https://ssrn.com/abstract=3630700.

Schmitt, M. & Vihul, L. (2017). Politicized: The UN GGE's Failure to Advance Cyber Norms. *Just Security online forum*. Retrieved from https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.

Schmitt, M. (2020a). Taming the Lawless void: Tracking the Evolution of International Law Rules for Cyberspace, *Texas National Security Review,* Volume 3, Issue 3 (Autumn 2020).

Schmitt, M. (2020b). Israel's Cautious Perspective on International Law in Cyberspace: Part I (Methodology and General International Law). *Blog of the European Journal of International Law*. Retrieved from https://www.ejiltalk.org/israels-cautious-perspective-on-international-law-in-cyberspace-part-i-methodology-and-general-international-law/

Schondorf, R. (2020). Israel's perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations. *Blog of the European Journal of International Law*. Retrieved from https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/.

Strickling, L. E. & Hill, J.F (2018). Multi-stakeholder Governance Innovations to Protect Free Expression, Diversity and Civility Online. In: Donahoe E., Hampson F.O., (ed.) Governance Innovation for a Connected World – Protecting Free Expression, Diversity and Civic Engagement in the Global Digital Ecosystem, (special report), Centre for International Governance Innovation, Stanford Global Digital Policy Incubator.

Swire, P. (2016). The Data Protection Commissioner and Facebook Ireland Limited and Maximillian Schrems, Affidavit of Peter Swire. *SSRN Electronic Journal*. Research Paper No. 18-2. Georgia Tech Scheller College of Business. Retrieved from https://ssrn.com/abstract=3097444

Swire, P. and Kennedy-Mayo, D. (2022) The Effects of Data Localization on Cybersecurity (February 9, 2022). Georgia Tech Scheller College of Business Research Paper No. 4030905, Retrieved from: https://ssrn.com/abstract=4030905 or http://dx.doi.org/10.2139/ssrn.4030905

The White House (2022). *FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework*. Retrieved from https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/

The World Summit on the Information Society (2015a). *Basic Information: About WSIS.* Retrieved from https://www.itu.int/net/wsis/basic/about.html.

The World Summit on the Information Society (2015b). *WSIS Outcome Documents*. Retrieved from https://www.itu.int/net/wsis/.

U.N. Secretary-General (2013). *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.* Retrieved from https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/66/PDF/N1337166.pdf?OpenElement.

U.N. Secretary-General (2015). *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. Retrieved from https://digitallibrary.un.org/record/799853.

U.S. Department of State (2022). *Declaration for the Future of the Internet*. Retrieved from https://www.state.gov/declaration-for-the-future-of-the-internet.

U.S White House, *U.S.-E.U. Trade and Technology Council* (2021). *U.S.-EU Summit Statement*. Retrieved from https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/15/u-s-eu-summit-statement/.

United Nations Office for Disarmament Affairs (2022). *Developments in the field of information and telecommunications in the context of international security*. Retrieved from https://www.un.org/disarmament/ict-security/.

United States Department of State (2022). *A Declaration on the Future of the Internet*, Retrieved from: https://www.state.gov/declaration-for-the-future-of-the-internet.

World Economic Forum (2022), Global Risk Report, retrieved from: https://www.weforum.org/reports/global-risks-report-2022/

**Amit ASHKENAZI**

Law and Technology Expert, Adjunct Lecturer, Haifa Center for Law and Technology.

Amit Ashkenazi is a law and technology expert consulting public and private organizations on cybersecurity, Artificial Intelligence, Data Protection, and compliance and risk management.

Amit has been active in law, technology and policy issues in the Israeli government since 2002, covering Copyright law, Data Protection and Privacy, Electronic signatures, E-government, and Cybersecurity, and has represented the Israeli government in the Israeli Knesset, and in the international sphere. Between 2014 and 2022 Amit was the first legal advisor of the Israeli National Cyber Directorate, and developed and deployed the Directorate's domestic and international legal policy, as well as setting up and managing the INCD legal department.

In 2019 Amit represented Israel in the drafting of the OECD Recommendations on AI.

Before joining the INCD in 2014 to, Amit was Head of the Legal Department in the Israeli Law Information and Technology Authority in the Ministry of Justice (ILITA), now renamed The Privacy Protection Authority, Israel's Data Protection Authority. In this context he was involved in international data protection issues, including the EU Adequacy finding of Israel's Data Protection regime and in the OECD.

Since 2013, Amit teaches a graduate course on Law and Information Technology in the Center for Law and Technology in the Haifa University Faculty of Law, and, since 2021, also in the Tel Aviv University Graduate program on Cyber, Politics and Government.