Improving the practice of cyber diplomacy:

A gap analysis of training, tools, and other resources

FINAL STUDY

Stephanie Borg Psaila

December 2021

DiPLO
www.diplomacy.edu

Impressum

Improving the practice of cyber diplomacy:
A gap analysis of training, tools, and other resources – Final study

Publisher
DiploFoundation (December 2021)
www.diplomacy.edu
diplo@diplomacy.edu

Author and lead researcher
Stephanie Borg Psaila

Research support and contributions
Katarina Andjelković, Andrijana Gavrilović, Katharina Höne, Tereza Horejsova, Marília Maciel, Tanja Nikolic, Hannah Slavik

Design and layout
Viktor Mijatović, Aleksandar Nedeljkov

Acknowledgements
To all the respondents who participated in the survey, and to all external reviewers – thank you.

Disclaimer

This is an academic research report that was commissioned by the Global Forum on Cyber Expertise (GFCE) as part of its Global Cyber Capacity Building Research Agenda 2021. The project was funded by Global Affairs Canada and the research was conducted by DiploFoundation.

The information, interpretation and examples set out in this paper do not constitute official or informal opinions or positions of the GFCE, its Secretariat, its members and partners, or any government. Neither the GFCE nor its members may be held responsible for the use which may be made of the information contained therein.

Through the Global Cyber Capacity Building Research Agenda mechanism, the GFCE aims to identify and address knowledge gaps relevant to ongoing GFCE work and members' capacity building activities. For this research project, the topic was identified in 2020 by members of the CBMs/Norms Implementation and Cyberdiplomacy Task Force under the Working Group on Cybersecurity Policy and Strategy. More information about the Working Group can be found on the GFCE website.

Index

Executive summary

Cyber diplomacy, the conduct of diplomacy with respect to a state's interests in cyberspace, is too important to ignore. Yet, the participation of countries is far from ideal.

For some countries, diplomacy has adapted quickly, and cyber issues are now firmly on their diplomatic agendas. For other countries, especially developing countries and small states, there are several challenges linked to limited human and financial resources, which limit their participation and render them largely inactive in the cyber diplomacy policy space. Naturally, countries with limited resources are more likely to invest the few resources they have in what the country sees as more essential areas – and most often, cyber is not on that list.

Yet, many cyber issues transcend borders, and often prey on the weakest actors. Measures to protect against vulnerabilities need to be implementable – and implemented – everywhere. And no country should rise above the applicability of norms of state behaviour.

This study analyses aspects of capacity development to increase the engagement of every country, that is, the availability of training opportunities, tools, and other resources and their reach and take-up.

While we appreciate that technical training (such as how to set up a Computer Emergency Response Team) is extremely important, this study focuses mainly on the need for diplomats to engage in cyber diplomacy. By that, we mean the need to understand the cyber security aspects countries and organisations face, the laws that can address them, and how cross-border investigations work; how some countries engage in dubious activities to try to cripple each other's critical infrastructures, and how laws can be interpreted to justify this behaviour; the policy measures a country needs to undertake to bring its hospitals back online if they are attacked, and how other countries can assist; the foreign policy a country's ministry of foreign affairs (MFA) needs to develop for its diplomats to be guided by. The list goes on.

The survey we conducted as part of this study confirmed that training and tools are indeed available (whether there are thematic gaps is a slightly different story), but they are certainly not reaching everyone. The findings also uncovered the reasons why practitioners are often not taking any, or further, training, and why they were not making use of the whole range of tools available to help them in their cyber diplomacy work.

There are three main reasons. The first is simple: If they aren't aware of training and tools in the first place, they can't make use of them. The second is that even if practitioners know about existing training, they often do not have the financial means to enrol. The third is that practitioners are often too busy to spend time training or exploring tools and possibly not encouraged to do so.

We then used five case studies to look at good practices, identify gaps, and determine solutions. We based our recommendations on the findings, and on our own experience of training diplomats for close to 20 years.

When it comes to the recommendations, we've steered clear from one-size-fits-all suggestions, in the knowledge that practitioners, practitioners, providers, and funders all have different aims and needs.

For instance, a practitioner who has received a scholarship to undertake training should follow up with the training provider on how the training has impacted their work, or their institution's work, even in cases where there's no obligation for them to give feedback.

Providers should help instill a culture of institutional capacity development by incorporating this message in training programmes, such as during the feedback stage.

Funders should support practitioners in analysing what they really need, and involve providers in the process, as it can be more cost-effective in the long run. When analysing needs, the main goal of capacity development should be kept in mind: it's not only about what people learn, but how practitioners apply the knowledge in practice.

This report, which we're referring to as the 'Full study', is the culmination of two phases:

- *Phase I, completed in September 2021, concerning the availability of training opportunities and other types of support and their take-up.*
- *Phase II, completed in December 2021, which includes the idenfied gaps, and makes recommendations on how to close them.*

Chapter 1. Introduction

1.1 About this study

We live in an age that is shaped by rapid technological advancements. In the space of just a few years, artificial intelligence (AI) technology entered our homes and everyday lives through smart devices. Technology is in the service of medicine and healthcare. Goods and services produced thousands of kilometres away can be acquired instantly.

As with every other area of human progress, there's a dark side to this evolution. Guns can be printed at home. A child's virtual friend can mask an evil identity. Our laptops can be manipulated to conduct cyberattacks.

There are three main ways that countries make cyberspace safer and more secure: they bolster their own defences to get ready for cyberthreats, they deter others (both state and non-state actors) from engaging in unwanted activity, and they engage in diplomacy to advance their interests and values.[1]

Engaging in cyber diplomacy requires an appreciation of technology's potential and how it can be misused. It requires an understanding of how legal means can deter harm and preserve individual rights. It requires recognition of how a country's policies can be used to improve its people's wellbeing and its relations with other countries. More importantly, the practice of cyber diplomacy needs to be attuned and in sync with the rapid changes in technology and evolving trends.

For some countries, diplomacy has adapted quickly. Cyber issues are firmly on their diplomatic agendas, digital foreign policies are dedicated to cyber aspects, and tech ambassadors are being accredited to the world's main digital hubs.

For other countries, engaging in cyber diplomacy is a significant challenge. Limited human resources means that diplomats need to prioritise other pressing needs over cyber issues. Lack of financial resources means that diplomats are ill-equipped with the knowledge required to engage in discussions. As a result, some countries are unable to participate in cyber diplomacy, or lack the capacity to engage with it in meaningful or effective ways.

This study is concerned with the capacity development aspect of cyber diplomacy. It looks at the availability of training opportunities and other types of support and their take-up, identifies the gaps, and makes recommendations on how to close them.

Here are the steps taken to reach its conclusions:

- This chapter – Chapter 1 – provides context to identify the needs: who the cyber diplomacy practitioners are, where cyber diplomacy is conducted, and which countries are the most active and inactive. It also includes an explanation of the methodology used in this study.
- Chapter 2 presents the mapping exercise of available training, tools, and other resources available, and how they help diplomats engage in cyber diplomacy.
- Chapter 3 presents the findings of a survey and analyses how widely used these tools and resources are by diplomats around the world, with a focus on the countries and regions that are not as active in cyber diplomacy. It also identifies why practitioners' needs are potentially not being met.
- Chapter 4 presents five case studies to identify good practices in other diplomatic communities, and how they can lend a hand in the practice of cyber diplomacy.
- Chapter 5 recommends how to bridge the gaps in the provision of training and tools for supporting cyber diplomacy, and the gaps reaching diplomats who are tackling – or need to tackle – cyber issues as part of their agendas.

1.2 The notion and practice of cyber diplomacy

What we mean by cyber diplomacy

In recent years, the practice of diplomacy has extended to new policy areas, including cyber issues. This has given rise to the term cyber diplomacy – a term often used interchangeably between two main notions.[2]

The first is the conduct of diplomacy with respect to a state's interests in cyberspace; it looks at digital issues as a topic. State interests are generally identified in national cyberspace or cybersecurity strategies, and more recently, through digital foreign policies.[3]

The second refers to the use of digital (or 'cyber') means to conduct diplomacy. This is often referred to as digital diplomacy or e-diplomacy, and looks at digital technology as a tool,[4] or instrument.[5]

While there's a tendency to conflate these two very different notions, the former is a more commonly accepted definition,[6] and the focus of this study. Accordingly, cyber diplomacy includes the following:[7]

- Responsible state behaviour in cyberspace and confidence-building measures (CBMs).
- Protection of the internet's public core, and a country's critical infrastructure.
- Cyber conflict and warfare.
- Policy and measures related to network and information security.
- Cybercrime and mutual legal assistance.
- Digital or cyber foreign policies.

In this study, we take the term to mean the practice of dealing with all these issues and more as a whole, rather than as distinct fields of practice.

The practitioners of cyber diplomacy

Basing our study on the notion that cyber diplomacy is the conduct of diplomacy with respect to a state's interests in cyberspace, the main actors in cyber diplomacy are as follows:

- MFAs responsible for pursuing a cyber diplomatic agenda, in close cooperation with other parts of government. In practice, this means diplomats and other officials within the MFA, including tech coordinators or ambassadors,[8] responsible for carrying out the MFA's agenda through bilateral or multilateral forums, and policymakers from other parts of government.
- Non-state actors, including the technical and industry sectors, academia, and civil society organisations, engaging with diplomats and policymakers in discussions or negotiations on cyber issues.[9]

Where cyber diplomacy is conducted

Cyber diplomacy discussions and negotiations take place through both bilateral and multilateral forums. Until 2018, there were over 200 bilateral agreements on cyber issues.[10]

On a multilateral level, most formal and informal bodies are now focusing on cyber issues. These include the following:[11]

- UN General Assembly, including the UN Group of Governmental Experts (UN GGE) and the Open-ended Working Group (OEWG) processes at the First Committee, and the Ad-hoc Cybercrime Committee at the Third Committee.

- UN system, including the UN Office for Disarmament Affairs (UNODA), the UN Office on Drugs and Crime (UNODC), the UN Institute for Disarmament Research (UNIDIR), and the International Telecommunication Union (ITU).
- UN processes, including the UN Roadmap on Digital Cooperation, and the 2030 Agenda for Sustainable Development.
- Regional bodies such as the European Union (EU), the Council of Europe, the World Trade Organization (WTO), the North Atlantic Treaty Organization (NATO), the Organization for Security and Co-operation in Europe (OSCE), the Organisation for Economic Co-operation and Development (OECD), the Asia-Pacific Economic Cooperation (APEC), the Association of Southeast Asian Nations (ASEAN), Organization of American States (OAS), the African Union (AU), the Shanghai Cooperation Organization (SCO), and the G7 and G20 countries.
- Other multistakeholder processes including the Paris Call for Trust and Security in Cyberspace, Tech Accord, Charter of Trust, and the Geneva Dialogue on Responsible Behaviour in Cyberspace, and broader initiatives such as the UN Secretary General's Roadmap for Digital Cooperation, and the Internet Governance Forum.

Countries that are the most active and inactive in multilateral cyber diplomacy

If we look at the geographical location of multilateral and regional bodies, based on their headquarters, and the countries that are active in UN cyber processes, we can immediately determine the world's multilateral cyber policy hubs. These include New York and Washington in the USA; Geneva, Brussels, and Paris in Europe; and Beijing in Asia. If we look at where the most active non-state actors are based, we can add Silicon Valley, Boston, Shenzhen, and Hong Kong to the global multilateral cyber policy map (Figure 1).

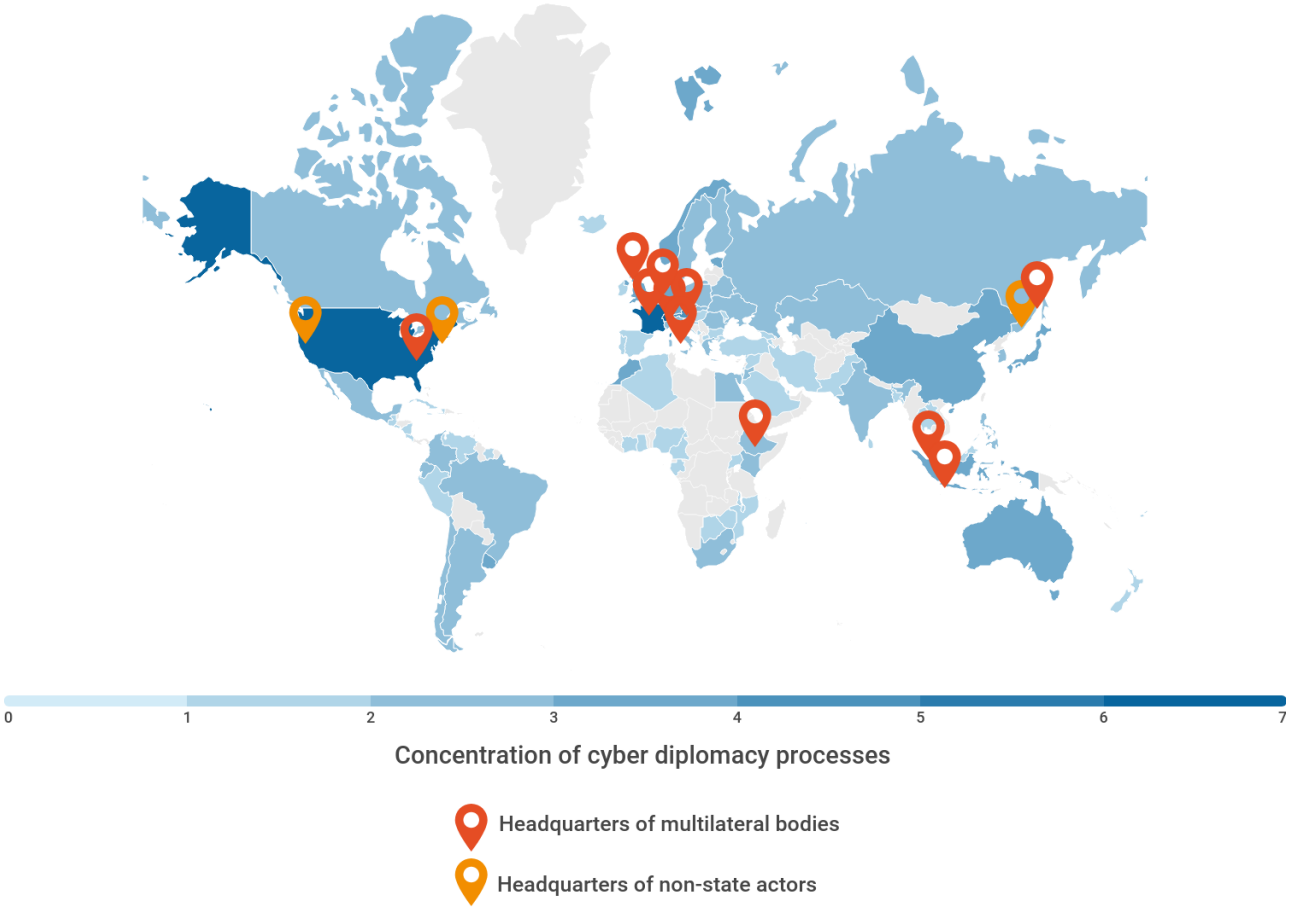


Figure 1. A multilateral cyber policy map, showing the countries that are most active in multilateral forums. Headquarters of multilateral bodies: New York (UN), Washington (OAS), Geneva (UN bodies), Brussels (EU, NATO), Strasbourg (Council of Europe), Paris (OECD), UK and Italy (current G7 and G20 chairs), Poland (OSCE), Addis Ababa (AU), Singapore (APEC), and Beijing (SCO). The headquarters of non-state actors, due to the high concentration of private actors: California (Silicon Valley), Boston, Shenzhen, and Hong Kong.

Capacity-related needs of practitioners of cyber diplomacy

There are at least two main broad dimensions that influence a country's engagement in policy processes: the political dimension and the functional dimension.[12] When adapted to the practice of cyber diplomacy, these translate to the importance a country attributes to cyber issues compared to other policy priorities (the political dimension), and the country's capacity to engage in discussions and negotiations on the issues (the functional dimension).

The countries most likely to be inactive in cyber diplomacy are generally those that consider cyber issues to be a low priority on their political agendas, and those that do not have adequate capacity to engage in cyber diplomacy.

Policy priorities and levels of capacity go hand-in-hand, and can affect each other significantly. If a country considers cyber issues to be high(er) on its priority list, it will consider it important to increase its capacity to engage in cyber diplomacy *(Figure 2)*.

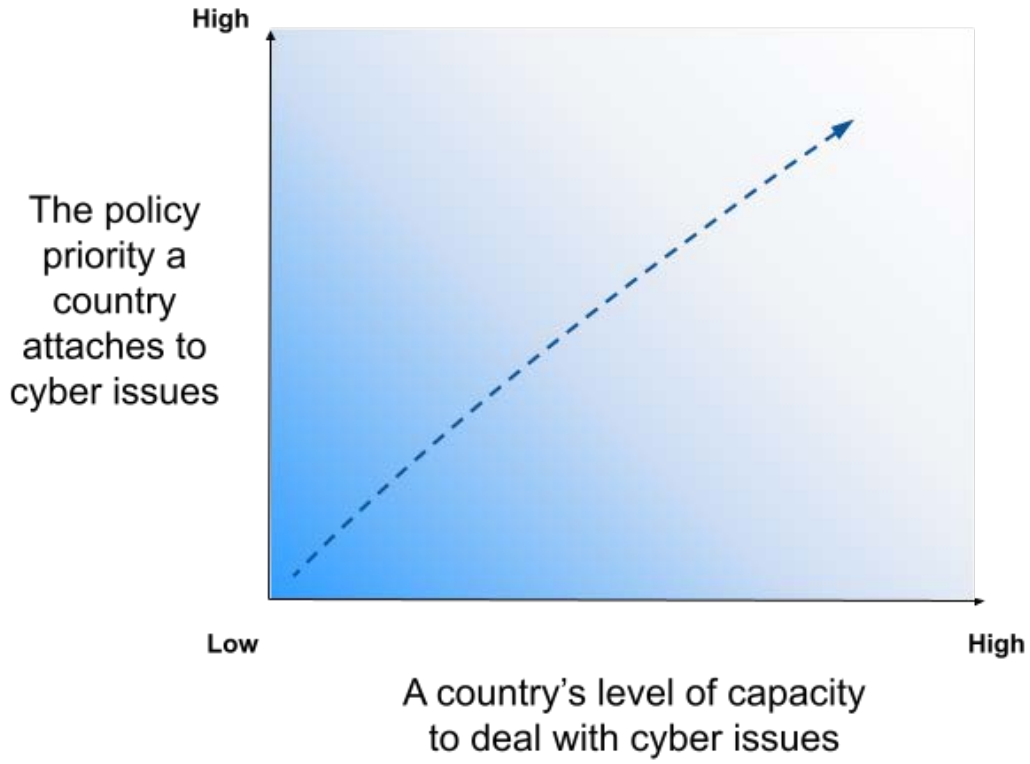


Figure 2. Enabling conditions for a country to be engaged in cyber diplomacy.

Conversely, however, a country that considers cyber issues as a low priority is also likely to not place importance on building its own capacities in the policy area. This affects not only that country (states that lack capacity will either be left out of negotiations and agreements, or receive them as a *fait accompli*[13]), but also everyone else. The notion that 'the weakest link is the biggest risk' is nowhere as true as in cyber issues. The challenge is that countries can easily fall into a vicious cycle *(Figure 3)*.

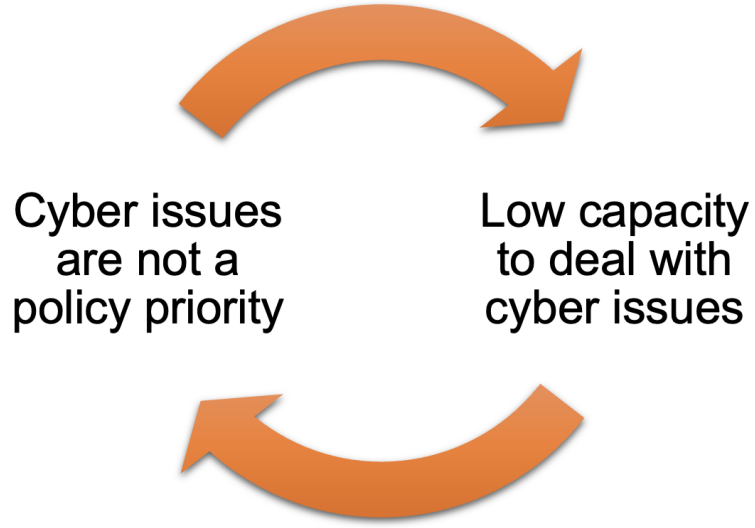


Figure 3. The vicious cycle of low priorities.

The main aims of building one's own capacity, therefore, are several. No matter how a country ranks cyber issues on its list of priorities, the wellbeing and safety of its citizens – offline and online – are generally a priority. This means having a resilient infrastructure and a system that deters cyber-wrongdoing. This is developed through technical and legal measures, backed by strategies that guide a country's internal work and foreign cooperation.[14] It also means that a country has the knowledge and skills to engage and cooperate with other countries to create effective regional and global measures. In brief, capacity development is a precondition for successful policy.

Capacity development needs to tackle both dimensions of engagement. In the political dimension, it needs to inform practitioners (especially policymakers) of the need for every country to be engaged; in the functional dimension, it needs to arm practitioners with the knowledge and skills to deal with cyber issues.

When it comes to developing capacity development strategies, these need to address competencies across four levels *(Figure 4)*.

Figure 4. The capacity development butterfly.

When adapted to the practice of cyber diplomacy, the following are some of the more specific needs each level (within a country) requires *(Table 1)*.

Table 1. The needs of cyber diplomacy practitioners.

Individual level	Explicit knowledge, including a basic understanding of how the internet functions, an advanced understanding of the policy issues (*What we mean by cyber diplomacy*), and advanced knowledge of the cyber diplomacy processes (*Where cyber diplomacy is conducted*). Soft skills and competencies (such as negotiation skills).
Organisational level	The knowledge to introduce cyber issues in foreign policies, or develop digital foreign policies. The capacity to secure the necessary human and financial resources. A culture of ongoing professional development and career advancement through training.
Institutional level	Expertise in technical, legal, and economic aspects of cyber issues. An advanced understanding of the political and functional dimensions of cyber issues. The capacity to secure the necessary human and financial resources. The knowledge to develop institutional and national policies.
Network level	A shared understanding of a country's national, regional, and global priorities.

The specific needs of small and developing countries

Small and developing countries face an additional set of challenges, lack of financial resources chief among them.

Smaller countries face the additional challenge of limited human resources. Typically, for instance, the work of a diplomat from a small state spans a broad range of topics. This is more acutely felt in permanent missions in New York and Geneva, where countries are represented by just a handful of diplomats.

There are also other challenges, such as limited or disrupted internet access, poor availability or use of technology, a knowledge deficit in other policy areas, and other pressing developmental issues (such as climate change issues for small island states) that take up significant resources to deal with.

Capacity development strategies need to keep the practitioners' environment in perspective, including all the challenges countries face on national, regional, and global levels.

1.3 Technical aspects of this study

Before we present the mapping exercise and the findings of our survey, here are a few technical details about the study, including its scope, definitions, methodology, and research design.

What's in scope, and what's not

The main aim of this study is to strengthen countries' ability to achieve higher levels of capacity, regardless of which level of priority they choose to attach to cyber issues. In practice, this study looks at what's available in terms of training, tools, and resources, as well as their take-up by the countries and regions who need them; what other types or forms of support can be made available; and short-, medium-, and long-term recommendations for bridging the gaps to meet the practitioners' needs.

It pays particular attention to the needs of small states and developing countries. Keeping in mind that there has never been a common definition that draws a clear line between small states and large states,[15] we define small states as those countries that fall within the 1.5 million population threshold[16] and those that share the characteristics of smallness.[17]

The same applies to the definition of developing countries. Due to the absence of a common definition, we base our definition on the taxonomies of the UN Development Programme (UNDP),[18] the World Bank,[19] and the International Monetary Fund (IMF).[20]

The global mapping on training takes a finite view in terms of the topics covered, and includes courses, workshops, and other types of training that deal exclusively or primarily with cyber diplomacy and the topics we consider to fall under this definition *(What we mean by cyber diplomacy)*, but excludes training that is not aimed at cyber diplomacy practitioners. Undergraduate studies are also excluded, since these are primarily aimed at students rather than practitioners. Regarding the types of training, the mapping includes face-to-face, virtual, and blended courses and workshops offered to practitioners *(The practitioners of cyber diplomacy)*, wherever they are based. Considering the small and finite variations of the term 'training', we consider the mapping of training to be comprehensive.

For our mapping on training, which we conducted between April and June 2021, we relied on the following:

- Inputs from Diplo's focus group on capacity development.
- Findings from studies on capacity development conducted by Diplo.[21,22]
- Data available on existing databases, the EEAS's Schoolmaster database of training opportunities and the UN Envoy on Technology's Database for Digital Capacity.
- Desk research based on publicly available online information.
- Data provided by respondents of both iterations of the survey.

The global mapping of tools and resources takes a practice-oriented approach to include toolkits and guidelines, collections of research papers and publications, and other sources of support – specific to cyber diplomacy – that help practitioners implement the knowledge in their practice of cyber diplomacy. Hence, while individual studies, reports, and articles certainly contribute to the body of knowledge, they are excluded from the mapping.

For our mapping of tools and resources, which we also conducted between April and June 2021, we relied on the following:

- Inputs from Diplo's focus group on capacity development.
- Data available on existing databases, including the Digital Watch observatory and the Cybil Portal.
- Desk research based on publicly available online information.
- Data provided by respondents of both iterations of the survey.

Methodology used in this study

This study tackles two distinct questions:

- What training and support is already in place, how widely used is it, and how can it be made more available?
- What's missing in cyber diplomacy training and support, and what can be developed, delivered, or provided?

The questions are addressed using an incremental approach and a gap analysis to identify existing capacity and use that as the foundation for moving forward.

With regard to data collection and analysis, we used a combined research methodology:

(a) We collated an initial set of mapping data through an in-house research focus group, complemented by desk research, as a primary source; and the use of existing databases as a secondary source.

(b) Using a sequential exploratory design, we used the initial data to develop a survey (a) for the collection of further data on existing training, tools, and resources; and (b) to identify variables that help determine how widely used the existing training and resources are, and to help determine the reasons for a high/low take-up. The survey was open to anyone who identified her/himself as a practitioner of cyber diplomacy. A total of 48 respondents took part in this phase.

(c) Using a sequential explanatory design, we used the findings from the first iteration of the survey as input for the mapping exercise, and as a fine-tuning for a second iteration (Annex I). A total of 77 respondents took part in this phase, bringing the number of **respondents who took part in the survey to 125**.

(d) The survey was anonymous, but provided the option for respondents to sign up for updates. More than half of the respondents provided their email address.

(e) Both iterations of the survey used conditional skip logic, which allowed respondents to skip to a later page based on their answer to a previous closed-ended question. As a result, several questions in the figures appear as 'skipped', when in reality, those questions were simply not presented to respondents, based on what they had responded to in previous questions.

(f) Conditional skip logic was used with the following:

- Multiple choice questions - respondents who specified they were diplomats were asked specific questions related to their profession.
- Matrix/rating scale (a closed-ended question that asked respondents to specify more details about the training they undertook and tools they used) - depending on their answers, respondents were then asked reasons for undertaking/not undertaking training, and using/not using tools.

(g) We analysed five case studies from communities of practice as good practices, which served as an additional basis for a gap analysis. The case studies are based on Diplo's direct experience in working with diplomatic communities in different fields of practice.

(h) In conclusion, we used the findings from the mapping exercise, survey, and case studies as the basis for a gap analysis. The identified solutions and recommendations, as a result of this analysis, were validated by the research focus group.

An important basis for this study is the knowledge and expertise of the members of the research team, and the experience of the organisation (Diplo). The team members have years of experience in designing capacity development programmes for a wide range of stakeholders, including the diplomatic community. Diplo is informally recognised as the diplomatic academy for small states. The in-house specialisation in capacity development is captured in various ways, including a training course on Capacity Development (offered since 2013); research studies carried out in partnership with, or mandated by, various stakeholders; and articles, blogs, webinars, and podcasts, all of which are reflected in the inputs of the focus group throughout the preparation of this study.

Limitations of this study

The research relied on information that is online and public. In some cases, details were scarce, and it was often unclear whether some of the training programmes were still being offered. Closed training opportunities, or training programmes available by invitation only, were therefore not included, unless sufficient basic information was available online to the public. These limitations are indicative of the issues practitioners of cyber diplomacy face when searching for training opportunities. As the findings indicate, the lack of awareness of training opportunities is a significant barrier; recommendations for overcoming this issue are tackled in Chapter 5.

The research relied on information that was available only in English (regardless of the language used in the training). A limitation of this study is that the database of training and tools compiled as part of this study may appear US- and Europe-centric. There may indeed be additional training and tools in other languages which are not captured in this study. On the flipside, this creates an opportunity for similar studies to be carried out in other languages.

When it comes to the providers of training and tools, no public information was readily available on any training or tools offered by the private sector (see Figures 5 and 6 in the study). This could be due to the fact that training opportunities are offered directly to individuals or organisations, without the need for public announcements. The industry may also be contributing to programmes on topics which go beyond the definition of cyber diplomacy we adopted in this study. Lastly, the private sector may be involved as financial supporter, rather than the provider of the training or tool itself; information about supporting entities goes beyond the scope of this study.

Lastly, the case studies we used in this study are based on Diplo's experience in working with diplomatic communities in different fields of practice. This does not mean that these case studies are the only good examples; there are many others, possibly too long to list. However, the study utilises examples which the research team was able to describe with authority, based on direct, first-hand experience of working with these organisations.

Chapter 2. Mapping existing training, tools, and other resources

2.1 Cyber diplomacy training

Through our mapping exercise, we identified 28 training programmes in cyber diplomacy. **The full database can be found in Annex II.**

The programmes in the mapping include **courses** (where the main methodology involves reading modules and asynchronous activities); **workshops** (where activities are predominantly synchronous, such as lectures or discussions); and **mentorships** (where participants shadow the work of more experienced practitioners). Typically, workshops range from one to several days in duration; courses (excluding Master's programmes) range from 2 to 10 weeks in duration. Most of the training is offered online.

Note that in this section, we use codes (Tr) for each training programme. The codes and full names are also listed in Annex II. For details on methodology and sources, see *Technical aspects of this study*.

(a) By stakeholder group

The mapping looked at training developed and/or delivered by providers from every stakeholder group. The identified training programmes are offered by **academia, civil society and think tanks, governments, and intergovernmental organisations (IOs)**. Training offered by diplomatic training academies within MFAs was excluded, since information about such training is very often available only internally within the MFA.

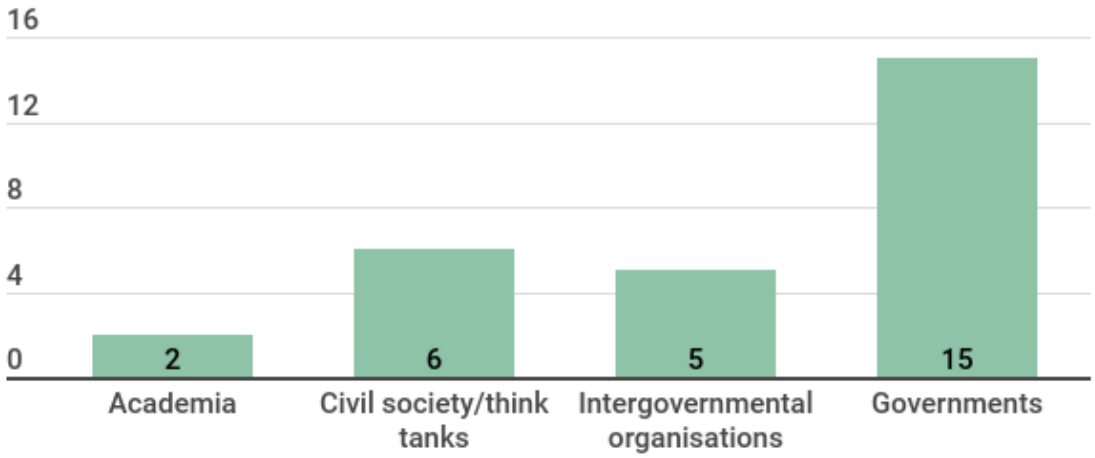


Figure 5. The number of training programmes per stakeholder group.

Most programmes are offered by IOs, headquartered in Europe. These include IOs in Geneva (UNIDIR, UNITAR), Paris (OSCE), Tallinn (NATO CCDCOE), and Vienna (UNODA).

A small number of programmes are offered by IOs in collaboration with other government or national partners. This allows programmes to be tailored to the regional and local needs of participants.

(b) By topic

The training programmes included in the mapping were those that tackle at least half of the topics falling under the term cyber diplomacy (*What we mean by cyber diplomacy*), that is, cyber diplomacy processes at UN and other multilateral bodies, threats and vulnerabilities, norms of state behaviour, the application of international law; CBMs, international cooperation, and broader contexts (Table 2).

The mapping therefore excluded training that deals exclusively with cybersecurity aspects, or is of a purely technical nature. Training on cybersecurity strategies, information security, incident responses, business strategies, forensics, computer engineering, or other science or technical specialisations is therefore not included in the database.

Table 2. The topics tackled by training programmes according to stakeholder group.

	Acad.	Gov.	IOs	CS/TT
Processes at UN and multilateral bodies				
Threats and vulnerabilities				
The application of International Law				
Norms of state behaviour				
CBMs				
Capacity building				
Regional and international cooperation				
Broader contexts				

CBMs and cyber capacity building feature the least in cyber diplomacy training, especially in the programmes offered by IOs.

With regard to the training topics, while the programmes offer a mix of theoretical knowledge and practice skills, very few include opportunities to gain experience first-hand, such as through immersion activities.

(c) By target audience

The mapping looked at all training programmes offered to practitioners (*The practitioners of cyber diplomacy*) wherever they are based. Most programmes are offered to a broad range of practitioners working in policy and decision-making, with diplomats listed as a target recipient of the training. Only one training (Tr3) is offered specifically to diplomats.

As for the target region, around half of the programmes target practitioners anywhere they are based. The other half is offered to practitioners at regional or national levels.

(d) By modality

Table 3. The modality of training programmes according to stakeholder group.

	Type of training	Modality
Academia	Accredited Master's programme, or credits as part of the programme (Tr1, Tr2)	Face-to-face (Online during COVID-19)
CS/TT	Mostly courses (Tr4, Tr5, Tr6, Tr7)	Mix of online and face-to-face (held online during COVID-19)
Governments	Workshops; some programmes also include mentorship (Tr11, Tr12)	Mix of online and face-to-face
IOs	Mostly workshops; very few are courses	Mix of online and face-to-face programmes (most of which were held online during COVID-19). Online courses are typically self-paced.

Although several programmes were already being delivered online, through either a learning platform or a virtual meeting platform, most programmes shifted to an online format due to COVID-19 (Table 3).

Only two of the training programmes (Tr11, Tr12) included a policy immersion phase, that is, a dedicated time in the programme in which participants can observe practices and processes first-hand in the field, often by shadowing more experienced practitioners who serve as mentors.

2.2 Cyber diplomacy tools, resources, and other types of support

Our exercise identified 55 tools, resources, and other types of support. **The full database is available in Annex III.**

For details on methodology and sources, see *The technical aspects of this study*.

To follow a practice-based approach of tools for helping practitioners *implement* the knowledge in their own practice of cyber diplomacy, the mapping features three categories:

- **Collections of research and publications** (the collections or sources, rather than the individual research or publications).
- **Online databases** (broader repositories of information, which typically include actors, in-depth descriptors of the issues, events, and legal instruments) and **indices** (which rank countries based on a set of criteria or indicators).
- **Toolkits, guidelines, and manuals** (which offer actionable support in the form of how-to's).

The bulk of research and publications *(Figure 6)* comes from civil society and think tanks, as the drivers of analytical thinking on the issues. IOs are the main developers of hands-on resources, such as manuals and toolkits.

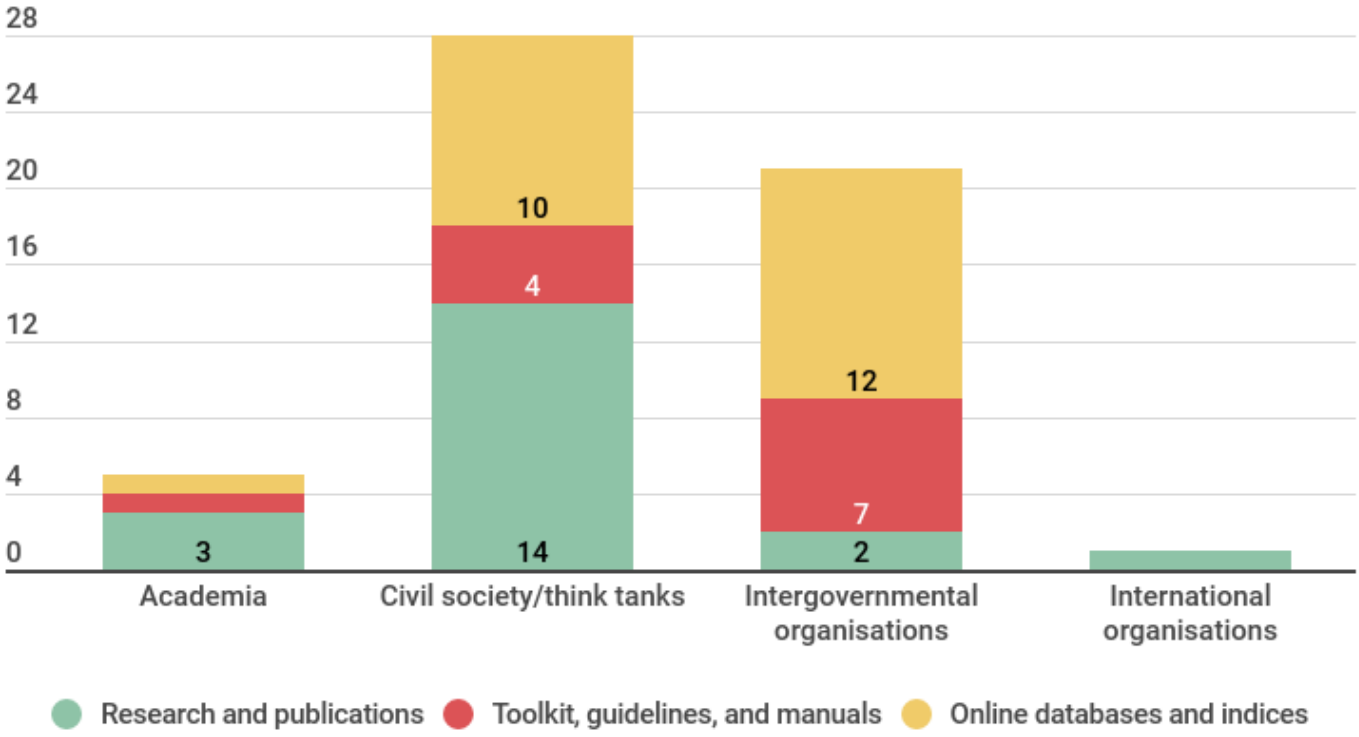


Figure 6. The types of tools per stakeholder group.

Chapter 3. Analysing the use of training programmes, tools, and other resources

3.1 The survey respondents

The analysis on the use of training programmes, and tools and resources, is based on the responses obtained from our survey, which we ran throughout June and July 2021. **A total of 125 respondents completed the survey, including 58 diplomats** *(Figure 7)*.

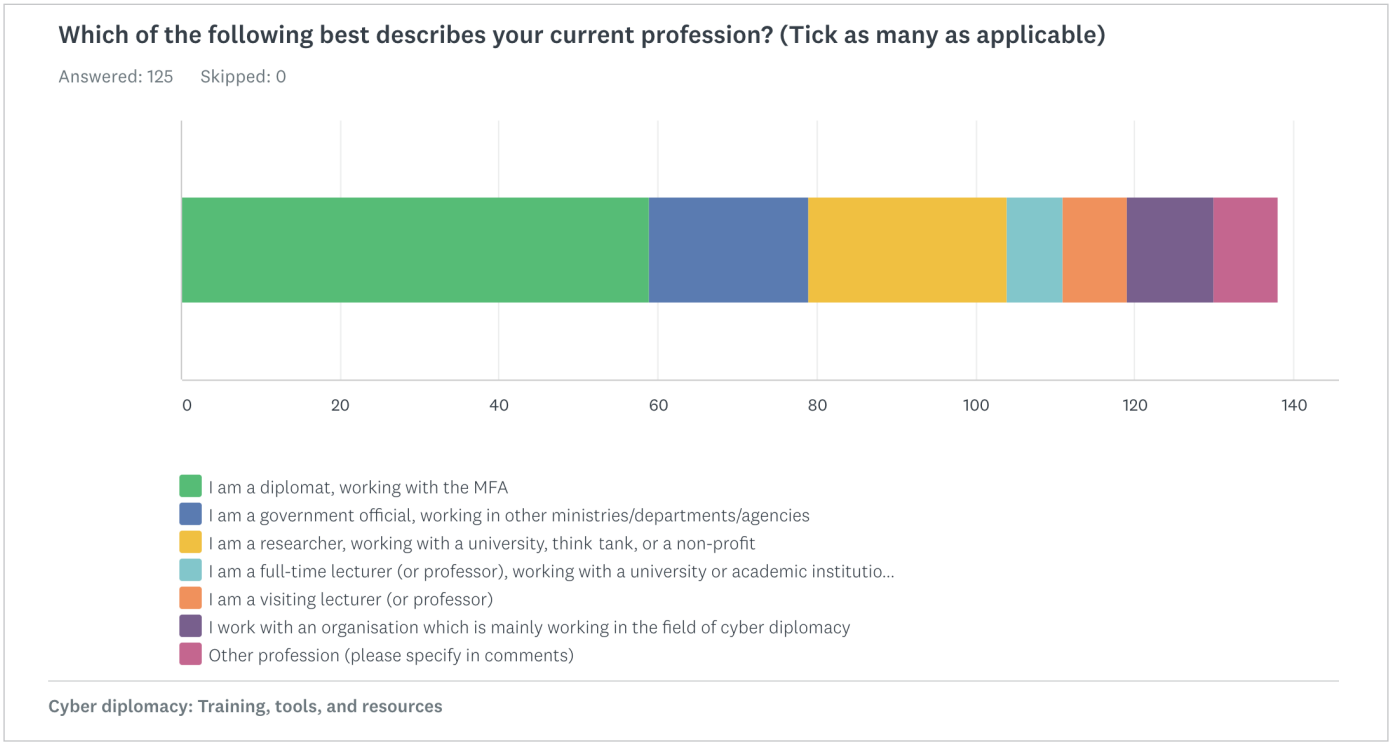


Figure 7. Profiles of the survey respondents.

Figure 8 gives an overview of the countries of origin of the 58 diplomats who responded to the survey.

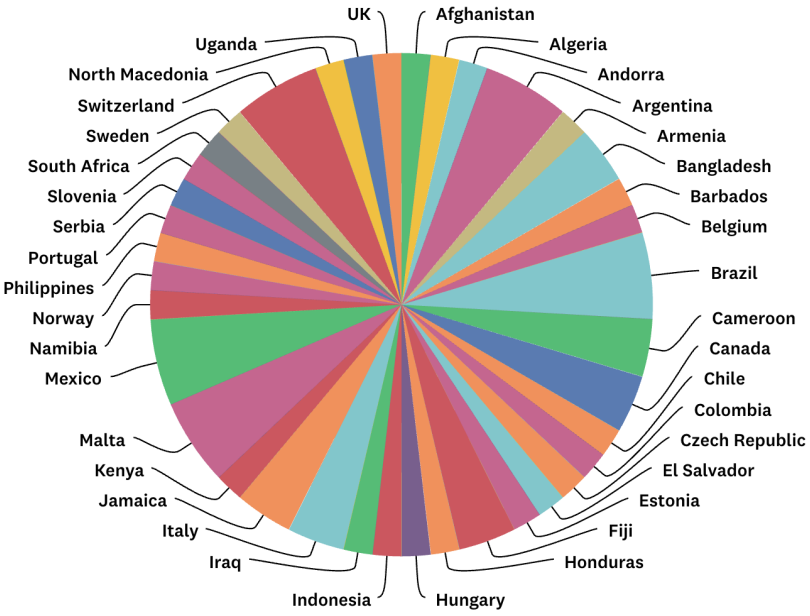


Figure 8. Countries of origin of survey respondents.

Of all the 58 diplomats (Figure 9), most respondents came from Argentina (3), Brazil (3), Malta (3), Mexico (3), Switzerland (3), Bangladesh (2), Cameroon (2), Canada (2), Fiji (2), Italy (2), and Jamaica (2).

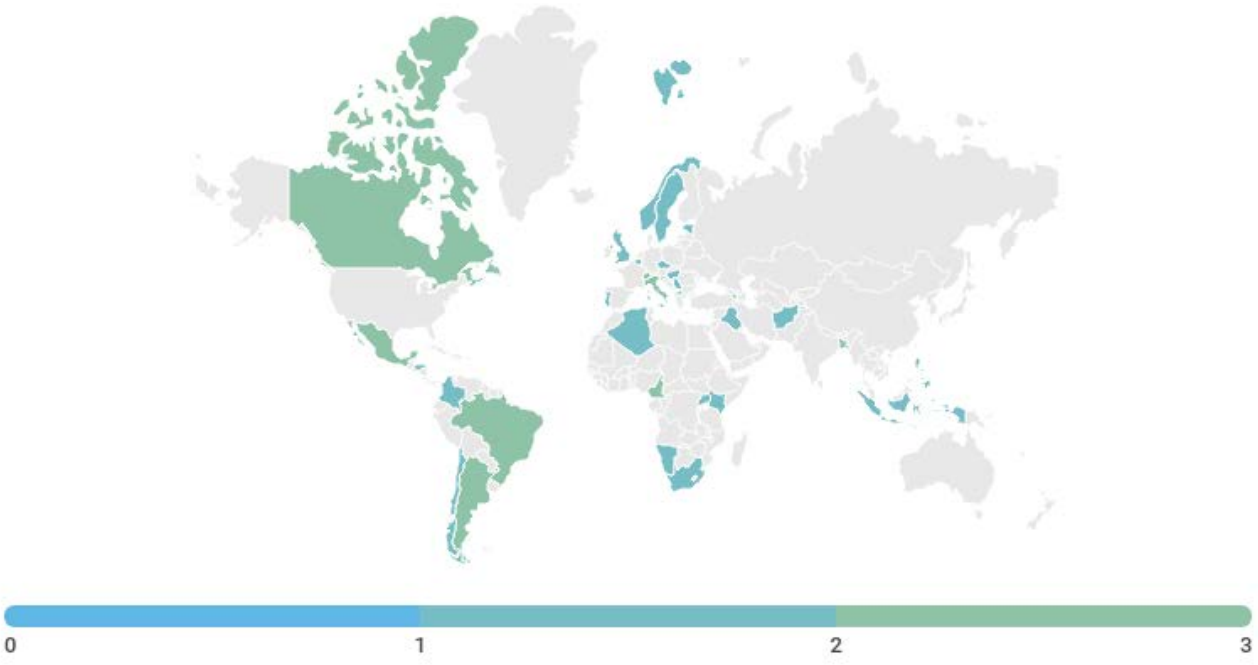


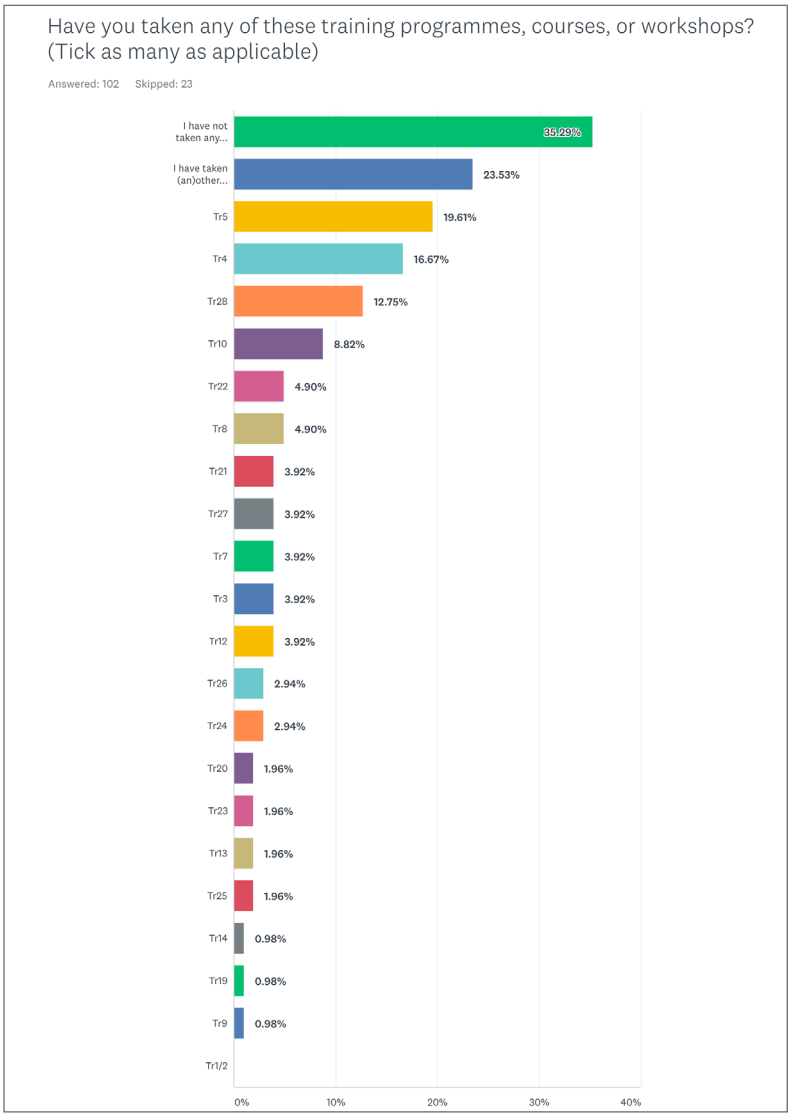
Figure 9. Countries of origin of diplomats who responded to our survey.

3.2 Analysing the take-up of training programmes

The survey provided all respondents with a list of training programmes to determine whether they were aware of them. From among **all the respondents**, almost two-thirds (65%) indicated that they had taken part in one of the programmes on the list or in other training programmes not included in the survey (Figure 10).

With regards to the second response, 'I have taken an(other) course not listed here', the courses are either internal MFA courses, or are programmes which are not specific to cyber diplomacy.

Figure 10. How all respondents replied to the survey question: Have you taken any of these training programmes, courses, or workshops?



An important finding is that just over one-third of all respondents (35%) – a relatively high percentage – indicated that they had not taken any training since starting working in the field of cyber diplomacy. The percentage is similar for diplomats: 31% indicated they had not taken any training.

Main reasons for not taking (other) training programmes

We asked both cohorts to indicate their reasons for not undertaking (other) training programmes. From among those who undertook training (and were therefore open to dedicating time for training), most said they were not aware of other programmes *(Figure 11)*.

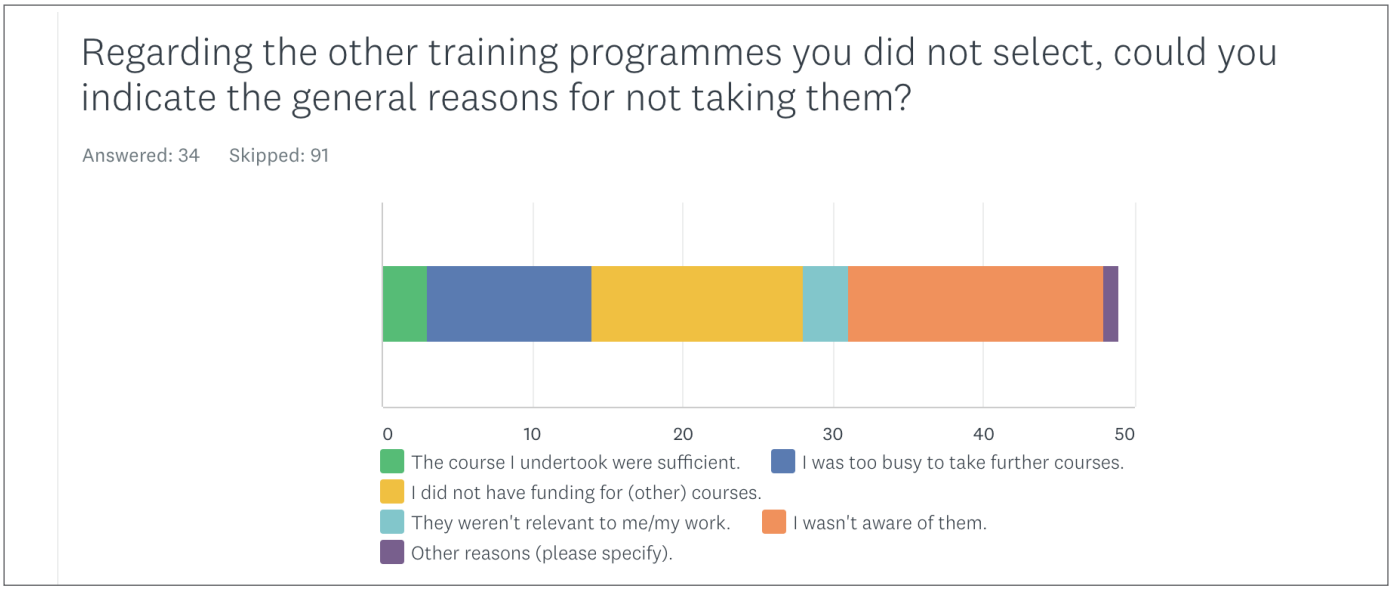


Figure 11. Responses to the survey question: Regarding the other training programmes you did not select, could you indicate the general reasons for not taking them?

From among the cohort who did not undertake any training at all, most replied that they were not aware of any training programmes *(Figure 12)*.

Figure 12. Responses to the survey question: Which experience best describes your reasons for not taking any training since starting your work in cyber diplomacy?

If we zoom into the replies provided by diplomats, similar findings emerge. Among the diplomats who undertook training (and therefore were open to dedicating time for training), most also said they were not aware of other training programmes *(Figure 13)*.

Figure 13. Diplomats who responded to the survey question: Regarding the other training programmes you did not select, could you indicate the general reasons for not taking them?

Among the diplomats who did not undertake any training at all, most also replied that they were not aware of any training programmes *(Figure 14)*.

Figure 14. Diplomats who responded to the survey question: Which experience best describes your reasons for not taking any training since starting your work in cyber diplomacy?

The findings confirm, therefore, that the main reason why practitioners do not undertake training is lack of awareness. The second and third most cited reasons are lack of funding and lack of time.

The lack of awareness of training opportunities was confirmed by other findings. Around one-third of all respondents (35% from all respondents; 35% from all diplomats) said that their workplace did not regularly share announcements about training opportunities with the staff. This conclusion was reinforced by the fact that the majority of respondents found out about training opportunities mostly through external networks they are part of, and emails they receive *(Figure 15)*.

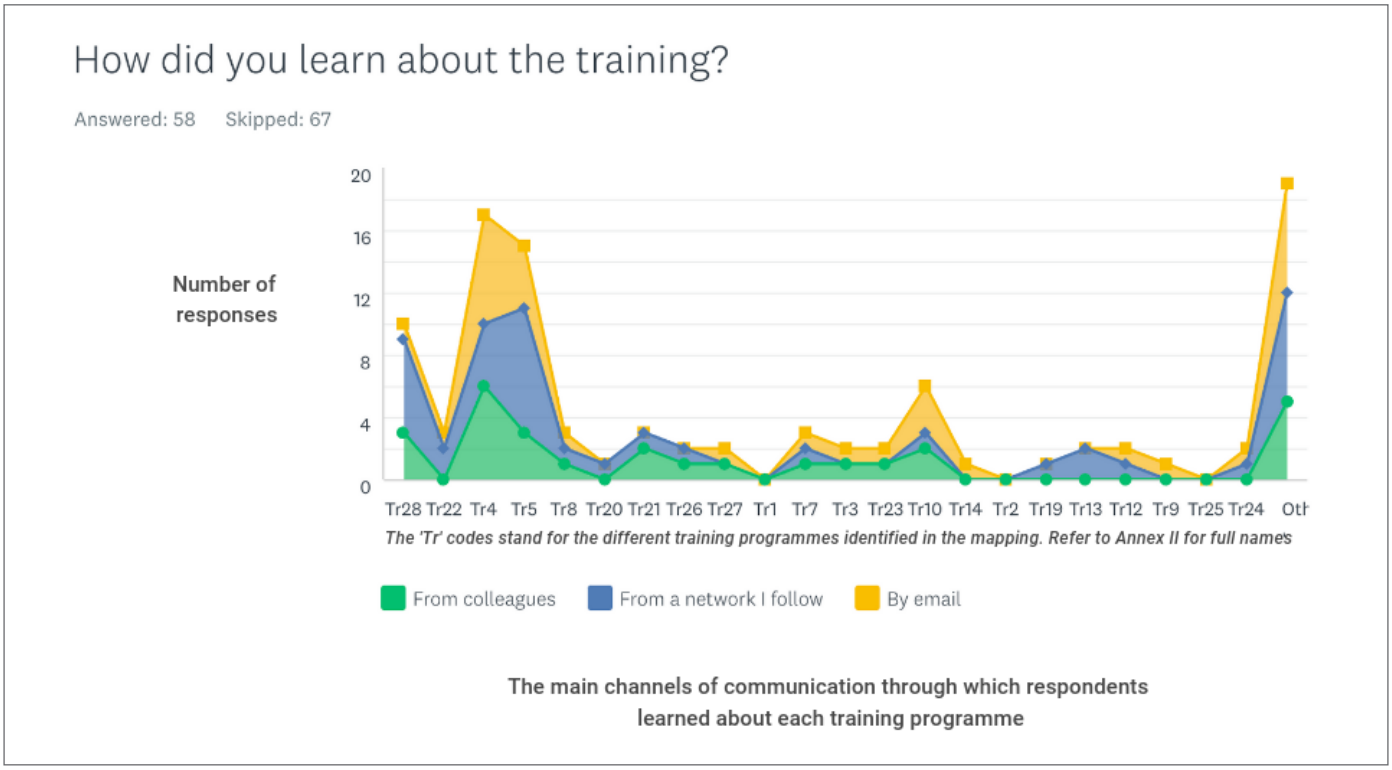


Figure 15. Responses to the survey question: How did you learn about the training? (Tr codes are explained in Annex II)

We also took a closer look at the second and third most cited reasons. We asked ourselves where the diplomats who felt they did not have the financial resources, hailed from. The findings show that 33% of diplomats were from small developing states; 17% were from a small developed state; while the other half (50%) was from developing countries. Especially with regard to respondents from developed countries, respondents may feel that it is the responsibility of their organisation to pay for training.

3.3 Analysing the reach and use of tools and resources

From the list of tools and resources presented in the survey (*What's in scope, and what's not*, and *The methodology used in the study*), the most widely used tools by the respondents are as follows (Figure 16):

- The ITU's resources, including the National Cybersecurity Strategies Repository, *Guide to developing a national cybersecurity strategy*, and the Global Cybersecurity Index – used by 82% of respondents.
- NATO CCDCOE's resources, including the Tallinn Manual, INCYDER database, and library – used by 71% of respondents.
- Diplo and the Geneva Internet Platform's (GIP's) Digital Watch observatory – used by 40% of respondents.

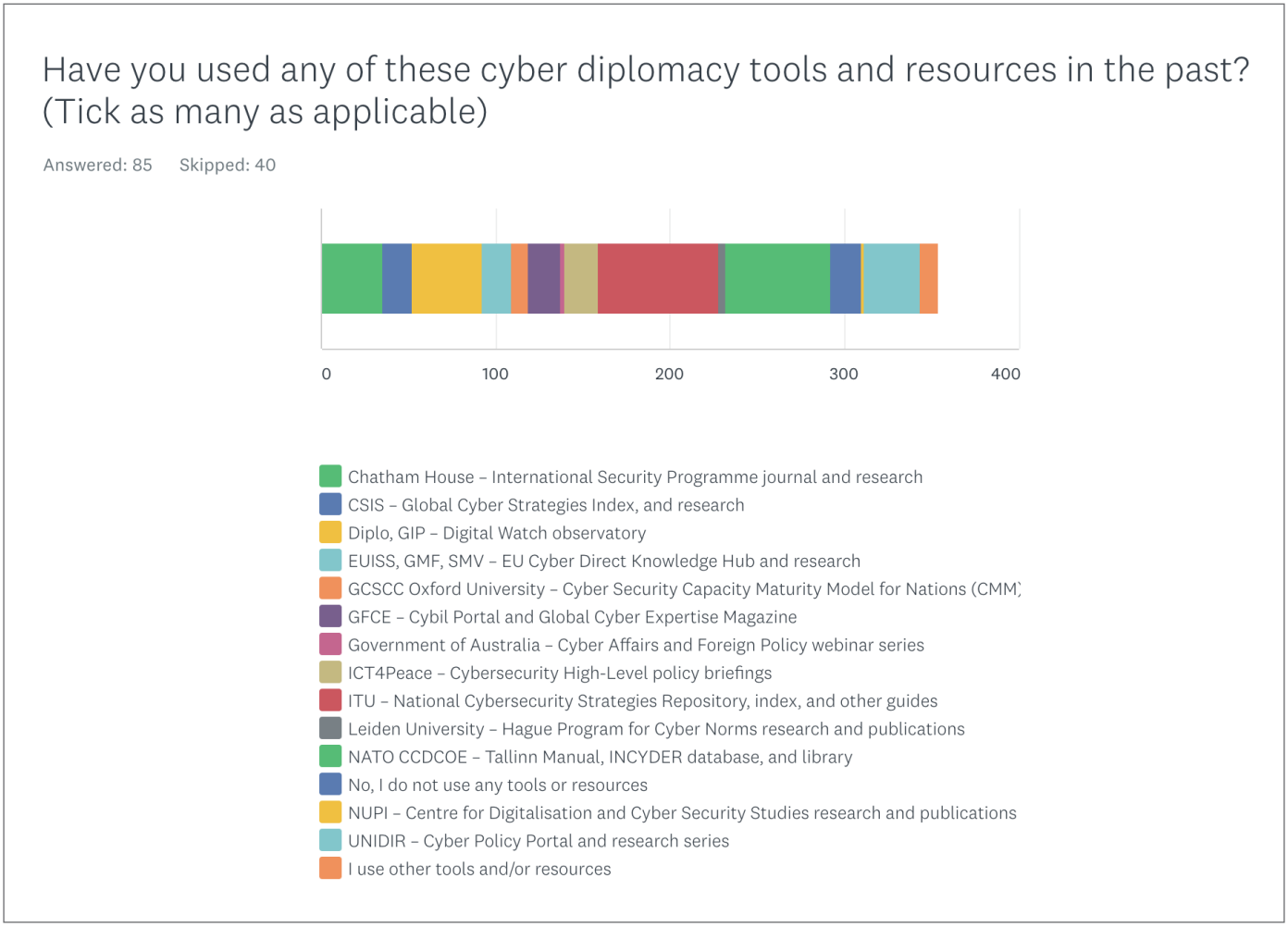


Figure 16. Responses to the survey question: Have you used any of the cyber diplomacy tools and resources in the past? (Note that respondents may have selected more than one tool)

The diplomats' use of the tools followed similar trends *(Figure 17)*:

- The ITU's resources – used by 19% of diplomats.
- NATO CCDCOE's resources – used by 21% of diplomats.
- Diplo and the GIP's Digital Watch observatory – used by 21% of diplomats.

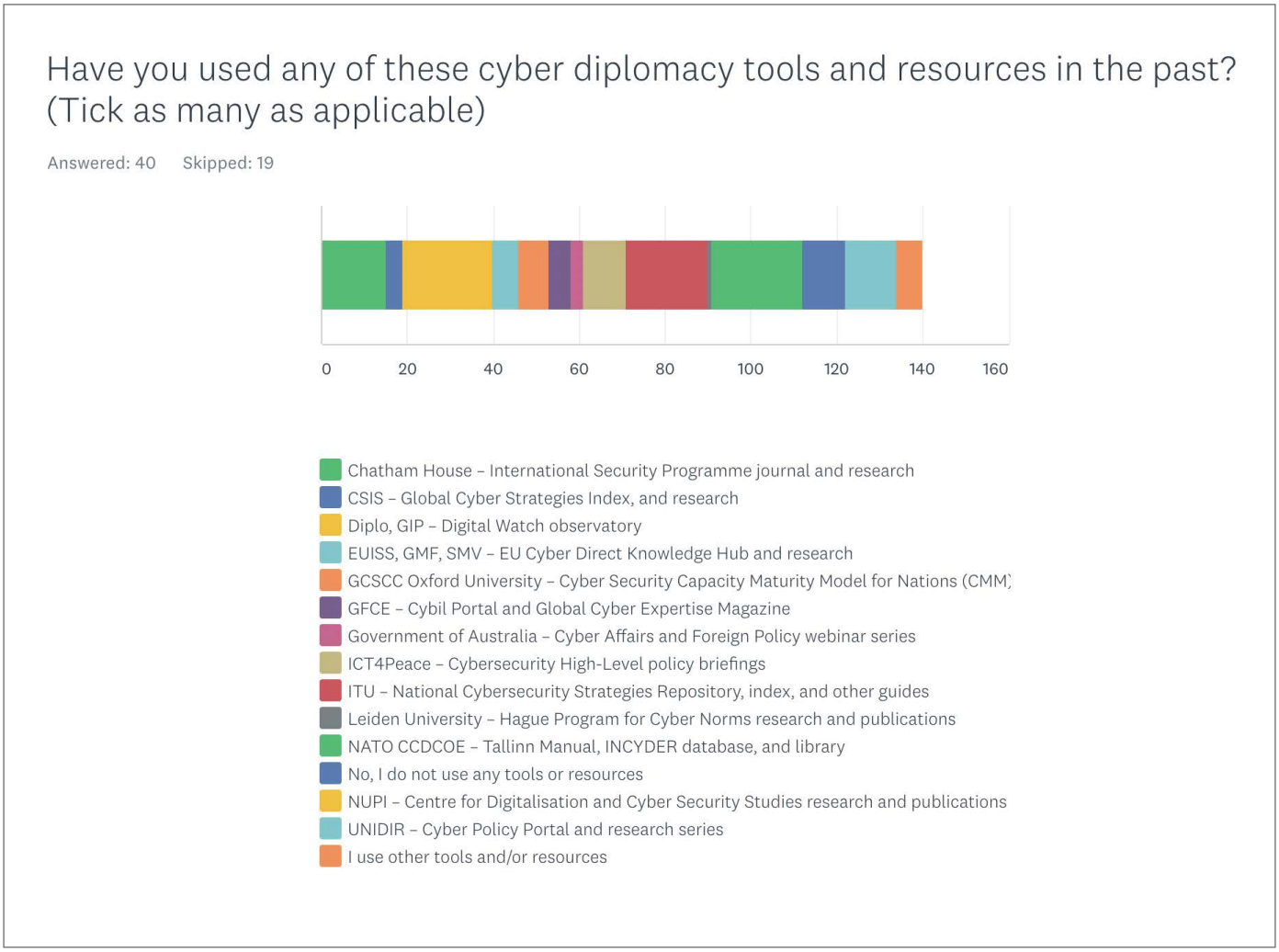


Figure 17. Diplomats' responses to the survey question: Have you used any of the cyber diplomacy tools and resources in the past?

Unlike training, in which 35% of all respondents and 31% of diplomats said they had not taken any training since starting their work in the field of cyber diplomacy, **only 21% (18 respondents) and 25% of diplomats (10 respondents) said they did not use any tools or resources as part of their work.**

Main reasons for not using (other) tools and resources

As we did for training, we asked all respondents why they did not make use of (other) tools and resources. From among the cohort who used other tools, 75% (30 respondents) said **they were not aware of other tools** *(Figure 18)*.

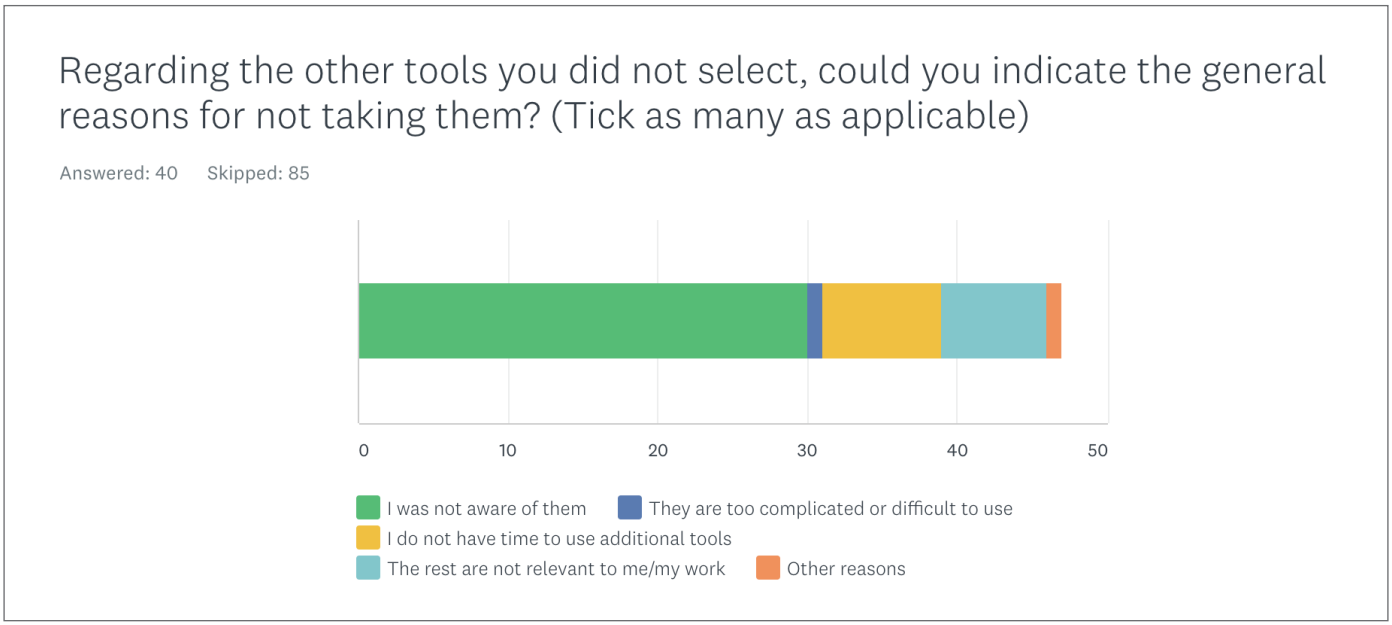


Figure 18. Responses to the survey question: Regarding the other tools you did not select, could you indicate the general reasons for not taking them?

The response is similar for diplomats, with 67% (10 respondents) saying they were not aware of the tools and resources *(Figure 19)*.

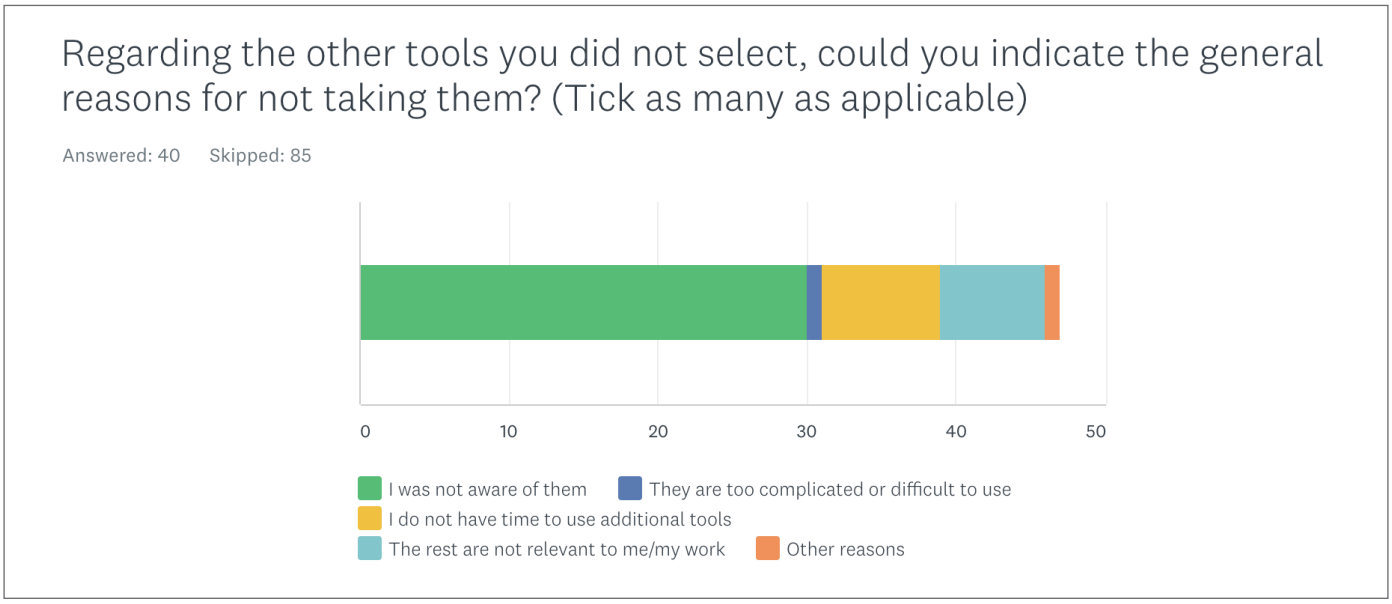


Figure 19. Diplomats' responses to the survey question: Regarding the other tools you did not select, could you indicate the general reasons for not taking them?

For respondents who said they did not use any tools and resources in their work (18 respondents – *Figure 20*; and 10 diplomats – *Figure 21*), the **main reason was also a lack of awareness**.

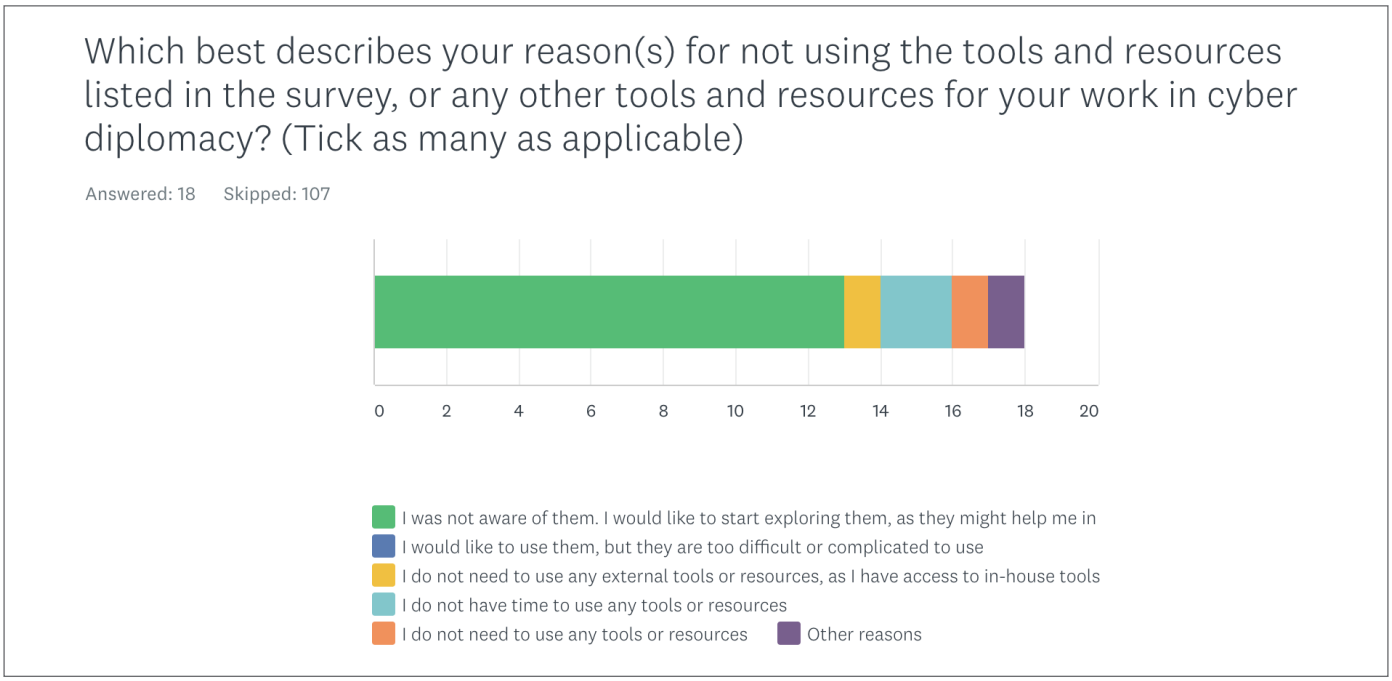


Figure 20. Responses to the survey question: Which best describes your reason(s) for not using the tools and resources listed in the survey?

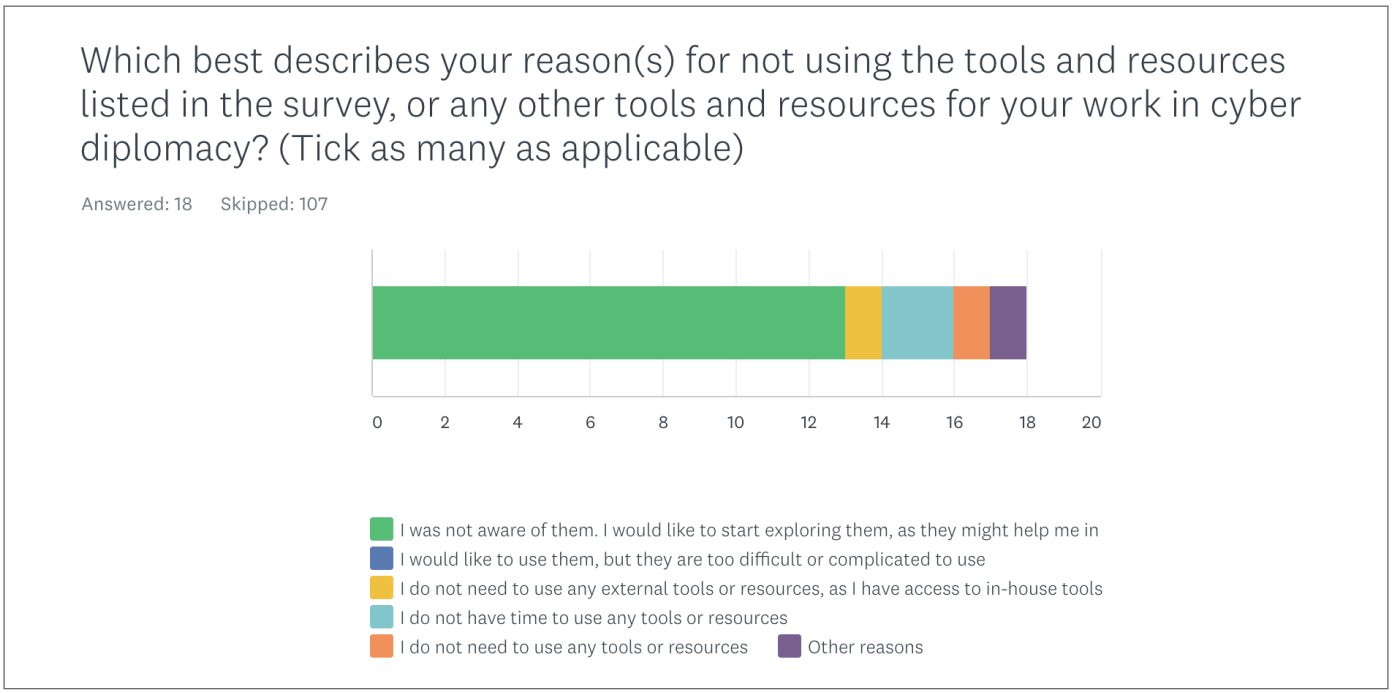


Figure 21. Diplomats' responses to the survey question: Which best describes your reason(s) for not using the tools and resources listed in the survey?

Chapter 4. Identifying good practices from other diplomatic communities

The survey results send a clear message: the most common reason for not making use of training and tools is because practitioners are not aware of them. Lack of financial resources to undertake training, and lack of time to dedicate to training, are also two common reasons why some practitioners are unable to undertake (further) training.

This chapter identifies good practices from other communities of practice, which show the impact that can result from exporting these practices to cyber diplomacy. Although the case studies are based on Diplo's direct and first-hand experience, our aim is not to talk about the training programmes themselves, but rather to highlight the major efforts and initiatives that other institutions have undertaken to build and improve the capacity development landscape.

4.1 Case study: Reaching out to small and developing countries

Diplo's online Cybersecurity course has been running since 2006. In the past 16 years, the 10-week course has been offered once a year for an average of 20 participants each year. That is roughly a cohort of 320 participants.

Based on feedback obtained from the course participants, most applicants first learned about the training from colleagues and through their workplace. From Diplo's end, the communications campaign for announcing an open call for applications emphasises **informing MFAs through established points of contact**.

Of all the alumni, 85% are from developing countries, and 9% are from small states (Antigua and Barbuda, Barbados, Cape Verde, Cook Islands, Dominica, Fiji, Guyana, Maldives, Malta, Mauritius, Niue, Saint Lucia, St Kitts and Nevis, Suriname, Togo, Tonga, and Trinidad and Tobago).

Almost half of the course alumni (46%) are government officials *(Figure 22)*. From among this smaller group, most alumni are diplomats, while the rest are officials from the ministries for communications and home affairs. A small number of alumni are from the security divisions of their governments.

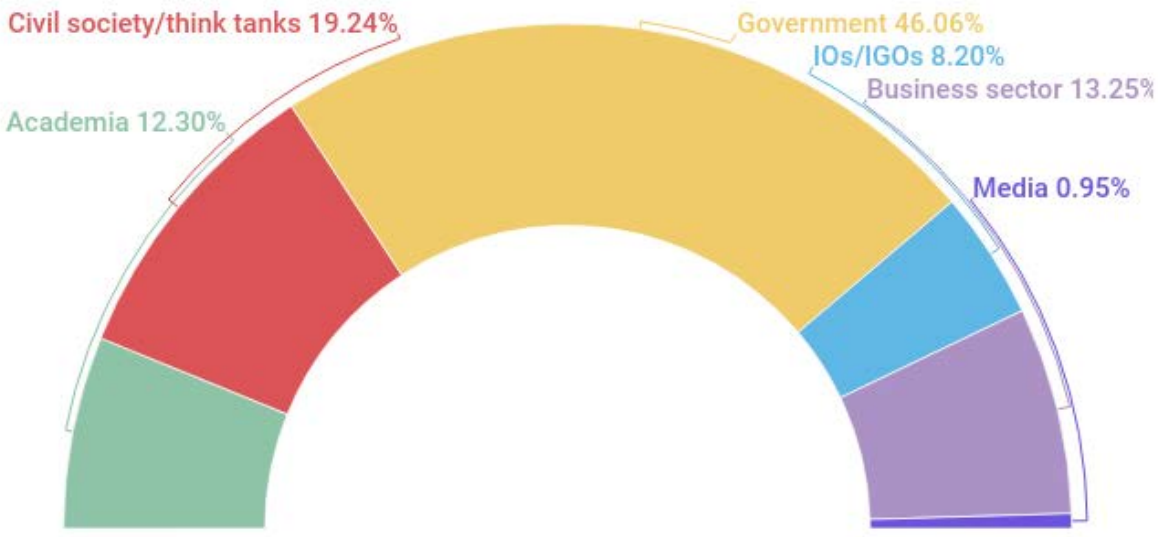


Figure 22. Stakeholder groups of alumni of DiploFoundation's online Cybersecurity course.

When it comes to the country of origin of the alumni from the government sector, most are from the Global South *(Figure 23)*. A small number of diplomats were on assignment at their country's Permanent Missions in New York and Geneva.

Figure 23. Countries of origin of alumni of DiploFoundation's Cybersecurity online course.

This case study shows that training programmes are certainly in demand, including in small and developing countries. Awareness of such training programmes, with the help of local entities, makes a big difference in the reach to, and the participation of, the practitioners who need them.

4.2 Case study: Awareness-raising through international networks

The training course on Humanitarian Diplomacy, launched in 2011 in collaboration with the International Federation of Red Cross and Red Crescent Societies (IFRC), is a good example of **how an international organisation can leverage its network of regional and national hubs to raise awareness about training**.

The 13-week online training quickly earned a reputation for being intensive and thorough (the training includes a 4-week research phase, where participants prepare a case study on a humanitarian diplomacy action relevant to their own work or area of interest), not least due to the involvement of IFRC's dedicated staff on the faculty team.

One of the main channels for sharing information about the training is **through the IFRC's network of national societies**, resulting in a large number of applications from humanitarian workers in the field (including with humanitarian NGOs). As a result, for each intake (twice a year), Diplo's receives 50% more eligible applications than the ideal number of participants for each course iteration.

4.3 Case study: Sustaining a scholarship fund

In 2015, the Government of Malta initiated a Scholarship Fund aimed at (a) participants from developing countries, and (b) participants from small states. Participants who apply for training with Diplo are eligible for a scholarship to cover the fees of courses related to diplomacy. Diplo uses the fund to provide partial (rather than full) scholarships, thus resulting in a larger number of participants benefitting from financial support.

Over the course of six years, 375 scholarships went to participants from developing countries *(Figure 24)*, including 107 scholarships for diplomats (or 29% of participants). The country of origins of these participants is quite extensive, and covers most of the Global South.

Figure 24. Countries of origin of scholarship recipients of the Malta Scholarship Fund.

A further 223 scholarships were awarded to participants from small states: Antigua, Bahamas, Barbados, Belize, Cape Verde, Fiji, Grenada, Guyana, Kiribati, Maldives, Malta, Mauritius, Nauru, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Samoa, Solomon Islands, Suriname, Trinidad and Tobago, and Vanuatu. Of the 223 scholarships, 183 (or 82%) were awarded to diplomats.

The total cost of the scholarship fund for these two groups – developing countries, and small states – has been €250,000. Over the course of seven years, **hundreds of diplomats – and their institutions – benefited directly from the financial support and training**.

4.4 Case study: Institutional support for staff training

Mexico's diplomatic corps is one of the largest in the world. The Ministry of Foreign Relations (MFR) has its own diplomatic training institute, the Instituto Matías Romero (IMR), founded in 1974.

The formal collaboration between IMR and Diplo goes back to 2009, when the governments of Mexico, Switzerland, and Malta signed a memorandum of understanding on diplomatic training. Under this agreement, which has been renewed multiple times, Diplo has trained more than 500 diplomats in contemporary diplomacy, funded by the Mexican government.

Back to our survey, the majority of diplomats (77% of the diplomats who responded to this specific question) said that their foreign ministry promotes career advancement through training *(Figure 25)*.

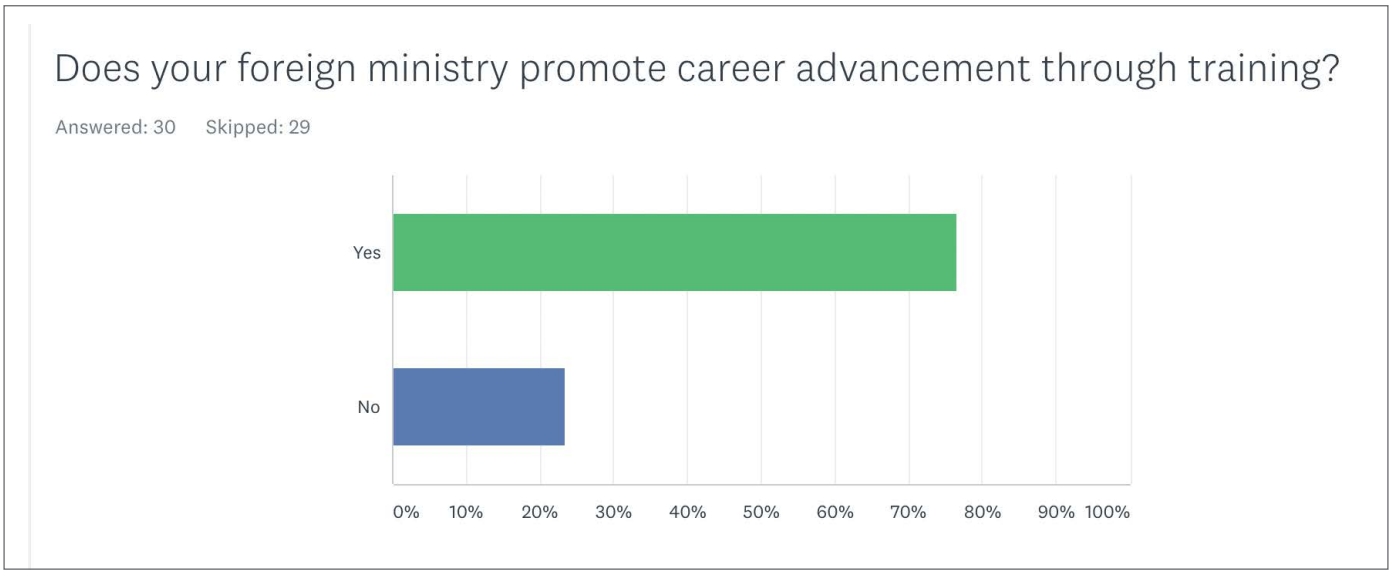


Figure 25. Diplomats' responses to the survey question: Does your foreign ministry promote career advancement through training?

But among that same group were diplomats who said they did not have funding (or did not get time off work to study) *(Figure 26)*.

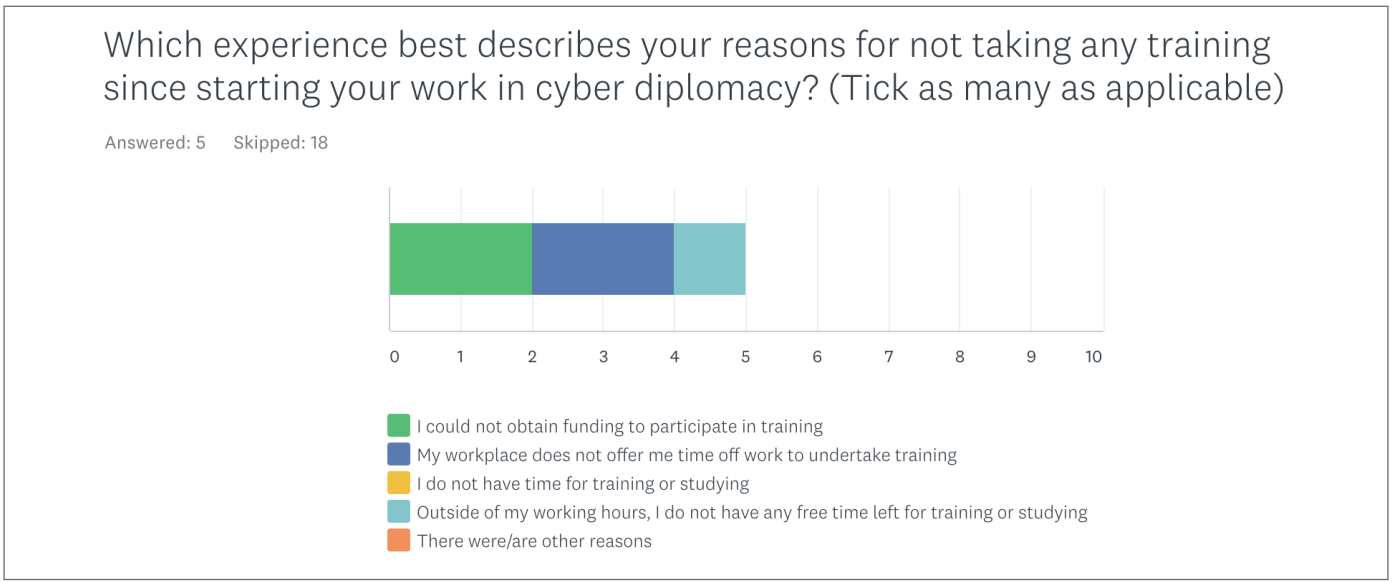


Figure 26. Diplomats' responses to the survey question: Which experience best describes your reasons for not taking any training since starting your work in cyber diplomacy?

This shows that although a culture of career advancement is important, it needs to be backed by measures that help diplomats undertake training in a practical way. In the case of Mexico's IMR – and across several other institutions that Diplo has worked with over the years – it is **by dedicating budgets for diplomats to pursue training in a sustained way.**

4.5 Case study: An immersive experience

Our fifth case study addresses an aspect that emerged from our mapping of training programmes: Hands-on policy immersion.

Among the aims of the Capacity Development Programme in Multilateral Diplomacy for Pacific Island States, a nine-month project in 2013–2014 funded by the Swiss Federal Department of Foreign Affairs, was to expose diplomats to the institutions and processes in Geneva whose decisions affect populations worldwide.

The 10 diplomats were able to see the operational side of multilateral diplomacy – from seeing first-hand the concentration of permanent missions and IOs, to holding roundtable discussions and simulations led by Geneva-based diplomats, to engaging with subject-matter experts in fields affecting the Pacific Islands.

The same programme ran again in 2016/2017, but was extended also to small and developing countries in the Caribbean and Africa. The immersion phase saw 16 diplomats who travelled to Geneva to familiarise themselves with the rich multilateral environment. No matter how well-designed a course is, **the benefits from on-the-ground experience cannot be replicated in ways other than in practice**.

De petits pays insulaires à Genève pour se frotter au multilatéralisme: An article by Stéphane Bussard for *Le Temps* (13 June 2017, in French)

© Mark Henley/Panos Pictures

Chapter 5. Recommended solutions to close the gaps

5.1 Improve the provision and take-up of existing training and other forms of support

Throughout this study, a guiding question was: How can existing training and support be made more available? The recommended solutions, based on our gap analysis of the three weaknesses which emerged from the survey, are directed individually at practitioners, providers, and funders. That's because one-size-fits-all solutions may not fully appreciate the different aims and needs of the actors involved.

Table 4. Recommendations for overcoming the issue of lack of awareness of existing training and tools.

The issue	**Lack of awareness of existing training and tools**
Gap analysis	It sounds counterintuitive that in this age of instantaneous and widespread communication possibilities, lack of awareness is one of the major barriers in the take-up and use of training and tools. Yet, we are bombarded with enormous amounts of information every day, which means that important messages can either fail to pass through the most effective communication channels, or can go unnoticed. There are two layers to this gap: lack of knowledge of the training and tools themselves, and lack of appreciation of the potential benefits of (online) training and tools. Based on the experiences from Case study 4.1 (Cybersecurity training) and Case study 4.2 (Humanitarian Diplomacy training), the first can be tackled as a logistical issue, mainly at the individual level; the second as a conceptual issue, mainly at institutional level.
Recommendations	*What can practitioners do?* • If you have taken any training or used any tools in your cyber diplomacy work, talk about it with colleagues and in your network. Others need to know about the benefits and your experiences. • If you haven't, reach out to peers from other countries directly or through a network, and ask your superiors. • If you're in charge of capacity development or human resources, make it your responsibility to keep track of national, regional, and global training opportunities that staff members can benefit from. *What can providers do?* • Establish contacts with MFA officials in charge of capacity development. • Provide information about your training or tool to coordinators of online repositories and databases, who can help amplify the opportunities. *What can funders do?* • Support online repositories and databases in their efforts to gather and maintain information about training. • Study thematic gaps in existing training, and functional gaps in existing tools.
A starting point	The Cybil Portal is a fully functional database of cyber-related projects, tools, and publications. Consider creating a space for listing training opportunities, and support an awareness campaign to promote it as a one-stop shop for cyber diplomacy capacity development. The portal will need resources to be updated and maintained.

Table 5. Recommendations for overcoming the issue of lack of funding.

The issue	Lack of funding to undertake training
Gap analysis	Lack of financial means is a well-known problem. One of the main reasons for this problem, confirmed through our mapping exercise, is that the cost of training programmes is often fixed for all and sundry. How can a diplomat from a least developed country (LDC) be expected to pay for a course that costs much more than their gross monthly salary, when the same course costs 10%–20% of someone's salary in a developed country? Scholarships certainly help with making training accessible. But the current levels of financial assistance going towards scholarships is not sufficient. Providers of training who receive financial support to offer scholarships are often faced with a difficult decision: Should the funds be used for partial scholarships (a higher number of participants, but still a challenge for those who are unable to source the rest of the funding), or full scholarships (providing full support, but assisting a much smaller number of participants)? In Case study 4.3 (scholarship fund), for instance, preference is given to partial scholarships, which means that participants, especially from LDCs, may still be missing out. Funders face challenges of a different nature. It's understandable for funders to want to gauge the real impact their money is having, before they decide to continue providing financial support, or to increase or diversify it. Providers are generally more focused on providing the training, and may view assessments as a heavy administrative burden. They might also not know how to ask for feedback, and how to present it to the funders. It circles back to funders: few are willing to provide extra support for impact assessments. Monitoring and evaluation is therefore often left to chance, rather than embedded into funding cycles.
Recommendations	*What can practitioners do?* • If you have benefited from financial support to undertake training, follow up with your provider on how the training has helped you or your institution improve aspects of your work. Talk about the impact derived from the training. You may not be obliged to do so, but your feedback can help ensure that funding remains available for other practitioners who need it. *What can providers do?* • Prioritise practitioners from LDCs, or countries that are largely inactive in cyber diplomacy (*Countries that are the most active and inactive in multilateral cyber diplomacy)*. • Realise that funders have reporting obligations, too. Integrating coursework and feedback into your training can instill a stronger culture of recognition of efforts. *What can funders do?* • When providing financial support, invest in impact assessment, incorporating this at the very start of the process (for instance, the application phase). • Appreciate that longer term capacity building support can be more impactful (for instance, it provides more certainty for providers, who can then plan their work along more ambitious medium- or long-term aims). • Provide funding for alternative and creative forms of support, such as twinning projects, which link institutions in developed countries to those in small and developing countries.
A starting point	Build on existing good practices, such as the Malta Scholarship Fund (Case study 4.3). Such initiatives can be scaled up by forging political and functional alliances between state and non-state actors.

Table 6. Recommendations for overcoming the issue of lack of time to dedicate to training.

The issue	Lack of time to dedicate to training
Gap analysis	The issue of professional development has been the subject of many debates among human resources, management, and capacity development experts. One of the reasons for lack of time is that employees feel they have too much on their plate. In reality, however, there will always be more work to do; the work is never quite done. In turn, employers are either caught up in the same conundrum (the department/ministry/entity cannot afford to spend time on training), or are at odds with how their employees are managing their time (thinking that lack of time is just a perception). When lack of time is confirmed by an organisation's senior staff, this is likely to be symptomatic of a deeply rooted problem – one that undervalues and underestimates the importance of capacity development. Limited time is different from no time. In fact, most training opportunities are based on the average time that a practitioner is able to dedicate to training. As our mapping exercise shows, many training courses are in the form of workshops, flexible online training, or other formats that deliver training in small nuggets.
Recommendations	*What can practitioners do?* • In entities without an official(s) dedicated to organisational capacity development, if you are a senior official in charge of human resources, make it your responsibility to learn about the benefits of training, not only on an individual level, but also at organisational and institutional levels. Training opportunities vary in duration and format, and offer participants a range of options to suit their needs. Appreciate that a little training is better than none at all. • Reach out to peers in other countries (such as Mexico, as in Case study 4.4) in which capacity development is an integral part of the MFA's internal policy. Training can be incorporated as part of a diplomat's familiarisation work, or linked to career progression. *What can providers do?* • Help instill a culture of institutional capacity development by incorporating this message in training programmes (such as during the feedback stage). • Provide as much flexibility as possible to participants, without compromising the knowledge-sharing goals of any programme. *What can funders do?* • Support dialogues on capacity development with senior staff of MFAs, with the aim of developing or strengthening internal policies on capacity development. • Support train-the-trainer programmes. Local trainers can champion organisational and institutional capacity development, resulting in stronger and broader impact.
A starting point	The International Forum on Diplomatic Training (IFDT) is an informal network of deans and directors of diplomatic academies and institutes of international relations. The fact that an MFA has a diplomatic academy is already a good indication that capacity development is valued as an integral part of a diplomat's work. This can be leveraged to encourage other MFAs to instill a culture of sustainable capacity development, through dialogues with the IFDT network.

5.2 Inform the development of new training and other forms of support

To answer the second research question – What is missing in cyber diplomacy training and support, and what can be developed, delivered, or provided – Tables 7 and 8 include a gap analysis based on areas of improvement identified through the analysis carried out as part of this study, and recommendations for practitioners, providers, and funders.

Table 7. Recommendations for overcoming knowledge and skills gaps.

The issue	Knowledge and skills gaps
Gap analysis	Based on our mapping exercise, there are two main gaps that create the space for improvement or provision of new training. The first relates to thematic gaps: CBMs and cyber capacity building do not feature prominently in training programmes offered by IOs. When it comes to broader aspects, only one programme deals with developing digital foreign policies – a new trend among foreign ministries that is fast becoming a prerequisite. More importantly, the second gap relates to skills. As noted in Chapter 2, very few training programmes include opportunities for participants to gain experience first-hand, such as through immersion activities. Case study 4.5 confirms that the soft skills participants acquire from being in the field are unparalleled to those offered by other formats. Immersion activities require significant funding, but the return on investment is for the benefit of the entire organisation and institution in the targeted countries.
Recommendations	*What can practitioners do?* • Analyse the capacity needed to determine the kind of tailored support you need from providers and funders to fit your organisational and institutional requirements, since your needs may change over time. If you need help with identifying what your organisation needs, ask peers, providers, funders, or other experts in the field for help. *What can providers do?* • Before undertaking new projects, or improving existing programmes, study the thematic gaps (for instance, by building on the findings of this study). • Offer training in soft skills. For instance, public speaking and the use of language in diplomacy are two often-underestimated skills. • Offer customised training. A one-size-fits-all approach can deliver theoretical knowledge, but customised training can help adapt the knowledge to local and regional contexts. *What can funders do?* • Support practitioners in analysing what they really need, and involve providers in the process. It can be more cost-effective to support a needs analysis, before funding the development of training, or providing financial support for practitioners. When analysing needs, the main goal of capacity development should be kept in mind: it is not only what people learn, but how practitioners apply the knowledge in practice. • Help fund training which focuses also on soft skills, and on policy immersion. • Focus on strategies that promote continuous and sustainable capacity development. There is value in supporting programmes year after year, as Case study 4.2 (Humanitarian Diplomacy training) shows.
A starting point	The GFCE's Clearing House plays a match-making role, connecting funders and providers to countries that request assistance. The Clearing House can be expanded to include cyber diplomacy capacity development.

Table 8. Recommendations for overcoming the gaps in the provisions of tools.

The issue	Gaps in the provision of tools
Gap analysis	There are undoubtedly a large number of tools available for cyber diplomacy practitioners. Many more are available in communities that focus on specific branches of cybersecurity, such as those related to national cybersecurity strategies, incident response, and other technical areas. There are two areas for improvement. The first is to improve existing tools. Databases, repositories, libraries, indices, and all other spaces which aggregate resources, for instance, need to be constantly maintained, both when it comes to outdated information, and also as new data becomes available. The second is to help scale up the existing landscape by developing new tools or types of support dedicated to specific regions or countries.
Recommendations	*What can practitioners do?* • Share any tools with peers or networks. A resource that is used by many practitioners is more likely to have the available support it needs to be maintained regularly. *What can providers do?* • Keep technological innovation in mind. New software can help present your information in smarter and more intuitive ways, making it easier on practitioners to access and utilise the information they need. The easier it is for practitioners to use your resources, the more widely used your resources will be. *What can funders do?* • Support local and regional variations of tools and other types of support. • Facilitate networking among providers of tools to avoid duplication of efforts. • Link providers of support to the private sector for additional support. As long as this does not influence the provider's mission and mandate, the assistance companies can provide NGOs, IOs, and governments (such as educational licences), can be a cost-saving incentive for fostering collaboration.
A starting point	There are several assessment toolkits for determining a country's capacity in certain cybersecurity areas (such as the capacity to combat cybercrime). These toolkits can serve as a model for developing a similar toolkit dedicated to capacity in cyber diplomacy.

Endnotes

1. Global Forum on Cyber Expertise [GFCE] (2019) *Towards effective cyber diplomacy: A guide to best practices and capacity-building* (white paper).
2. Riordan S (2016) *Cyber Diplomacy vs Digital Diplomacy: A Terminological Distinction*. USC Center on Public Diplomacy, May 12. Available at https://uscpublicdiplomacy.org/blog/cyber-diplomacy-vs-digital-diplomacy-terminological-distinction
3. Kurbalija J and Höne K (2021) *2021: The Emergence of Digital Foreign Policy.* DiploFoundation. Available at https://www.diplomacy.edu/sites/default/files/2021-03/2021_The_emergence_of_digital_foreign_policy.pdf
4. DiploFoundation (no date) 'Digital as a tool for diplomacy'. *Digital Diplomacy | E-diplomacy | Cyber Diplomacy.* Available at https://www.diplomacy.edu/e-diplomacy#ff1-3
5. Riordan S *op. cit.*
6. Barrinha A and Renard T (2017) 'Cyber-diplomacy: The Making of an International Society in the Digital Age'. *Global Affairs* 3(4–5), pp. 353-364. Available at https://www.tandfonline.com/doi/full/10.1080/23340460.2017.1414924
7. GFCE *op. cit.*
8. EU Institute for Security Studies [EUISS] (2021) *Cyber Diplomacy*. EU Cyber Direct. Available at https://eucyberdirect.eu/wp-content/uploads/2019/12/cd_booklet-final.pdf
9. Barrinha A and Renard T *op. cit.*
10. Based on ongoing research by DiploFoundation on cyber agreements.
11. Based on the list of actors involved in cyberconflict and warfare issues, available at https://dig.watch/actors/?issues=219&stakeholder_group=Intergovernmental
12. EuropeAid (2010) Toolkit for Capacity Development. *Tools and Methods Series*, Reference Document No. 6, European Commission. Available at https://europa.eu/capacity4dev/t-and-m-series/document/reference-document-nr-6-toolkit-capacity-development-2010
13. GFCE *op. cit.*
14. Painter C (2018) Diplomacy in Cyberspace. *The Foreign Service Journal* 95(5). Available at https://afsa.org/diplomacy-cyberspace
15. Psaila S (2010) *Small States at the United Nations*. Master's dissertation. Malta: University of Malta/ DiploFoundation.
16. Commonwealth Secretariat (1997) *A Future for Small States: Overcoming Vulnerability*. London: Commonwealth Secretariat.
17. Camilleri V (2007) 'The Definition of Small States'. *Diplomacy of Small States 0707*, Lecture 1, Introduction to Diplomacy of Small States. Malta: DiploFoundation.
18. United Nations Development Programme [UNDP] (2021) *Human Development Report 2020.* Available at http://hdr.undp.org/sites/default/files/hdr2020.pdf
19. The World Bank (2021) *The World by Income and Region.* Available at https://datatopics.worldbank.org/world-development-indicators/the-world-by-income-and-region.html
20. International Monetary Fund [IMF] (2021) *World Economic Outlook 2021: Managing Divergent Recoveries.* Available at https://www.imf.org/en/Publications/WEO/Issues/2021/03/23/world-economic-outlook-april-2021
21. Maciel M and Finlay A (2017) *Reviewing Global Internet Governance Capacity Development and Identifying Opportunities for Collaboration.* DiploFoundation. Available at https://dig.watch/sites/default/files/ITUIGreport2017newcover.pdf
22. Maciel M (2021) *Sustainable Capacity Building: Internet Governance in Africa*. DiploFoundation. Available at https://www.diplomacy.edu/sites/default/files/PRIDA_IG_sustainability_study_2021.pdf

Annex I

Survey questions

No.	Question	Notes
A	**Tell us about yourself**	
1	**Which of the following best describes your current profession? (Tick as many as applicable)**	
	I am a diplomat, working with the MFA	> Skip logic, Q2
	I am a government official, working in other ministries/departments/ agencies	> Skip logic, Q5
	I am a researcher, working with a university, think-tank, or a non-profit	> Skip logic, Q5
	I am a full-time lecturer (or professor), working with a university or academic institution	> Skip logic, Q5
	I am a visiting lecturer (or professor)	> Skip logic, Q5
	I work with an organisation which is mainly working in the field of cyber diplomacy	> Skip logic, Q5
	Other profession (please specify in comments)	> Skip logic, Q5
	Comments	
2	**Which country do you represent?**	
	[Drop-down list]	
3	**Are you working from your country's capital or are you currently serving abroad?**	
	Capital	
	Mission abroad	
4	**Does your foreign ministry promote career advancement through training?**	
	Yes	
	No	
5	**How long have you been involved in cyber diplomacy?**	
	[Date range]	
6	**Does your workplace regularly share announcements about training opportunities with the staff?**	
	Yes	
	No	
B	**Tell us about the following cyber diplomacy training:**	
7	**Have you taken any of these training programmes, courses, or workshops? (Tick as many as applicable)**	Choices randomised for each respondent
	ANU – Cyber Bootcamp Project	
	Clingendael – Cyber diplomacy training	
	Diplo – Cybersecurity	
	Diplo – Cybersecurity Diplomacy	
	ENISA – National Cyber Security Strategies (NCSS) workshop	
	ESDC – Cyberdiplomacy Tool for Strategic Security Policy	
	Estonian MFA – Tallinn Winter School of Cyber Diplomacy	
	Global Diplomatic Forum – Digital Diplomacy	

No.	Question	Notes
	Governments of AU, UK, CA, NL, and NZ with UNITAR – Women and International Security in Cyberspace Fellowship Governments of Australia and Denmark – Cyber and Tech Retreat ICT4Peace – Cybersecurity Policy & Diplomacy Workshops INCIBE and OAS – Cybersecurity Summer Boot Camp NATO CCDCOE – Executive Cyber Seminar NATO CCDCOE – International Law of Cyber Operations Norwich University – Cyber Diplomacy OSCE – Cyber/ICT security Confidence-Building Measures Course SELA – Specialisation Course on Cyber Diplomacy UNIDIR – Disarmament Orientation Course UNITAR – Digital and Cyber Diplomacy UNITAR – International Humanitarian Law and Cyber Warfare UNODA – Online Cyberdiplomacy Training Course UNSW Canberra at ADFA – Master of Cyber Security, Strategy and Diplomacy	
	I have taken (an)other training or course, which is/are not listed here. The institution and name of training programme(s) is/are:	Listed by respondent
	I have not taken any training since I started my work in cyber diplomacy	> Skip logic, Q11
8	**When did you complete the training?** [Date range]	Each training, including respondent's listed training from Q6, is listed for each response
9	**How did you learn about the training?** UNODA – Online Cyberdiplomacy Training Course - From colleagues From colleagues From a network I follow By email From an advert I knew about it From other sources, that is:	Each training, including respondent's listed training from Q6, is listed for each response
10	**Was the training free of charge?** Yes No; I paid for it No; I received a scholarship I prefer not saying	Each training, including respondent's listed training from Q6, is listed for each response
11	**Regarding the other training programmes you did not select, could you indicate the general reasons for not taking them?** The course I undertook were sufficient. I was too busy to take further courses. I did not have funding for (other) courses. They weren't relevant to me/my work. I wasn't aware of them.	

No.	Question	Notes
12	**Which experience best describes your reasons for not taking any training since starting your work in cyber diplomacy? (Tick as many as applicable)** The research I carry out as part of my work automatically equips me with the knowledge I need I was already fully qualified when I started my work in cyber diplomacy I was not aware of these (or other) training opportunities I could not obtain funding to participate in training My workplace does not offer me time off work to undertake training I am too busy at work to spare time for training Outside of my working hours, I do not have any free time left for training or studying I did/do not have the necessary prerequisite criteria to undertake training I could not/cannot travel (financial reasons, time limitations, VISA restrictions, etc) I do not have time for training or studying None of the training offers what I need or what I am looking for There is no point in training or studying, as it will not help me advance in my career There were/are other reasons, including:	
C	**Tell us about these cyber diplomacy tools**	
13	**Have you used any of these cyber diplomacy tools and resources in the past? (Tick as many as applicable)** C3SA – Cybersecurity Capacity Maturity Model for African nations (CMM) Chatham House – International Security Programme research and publications Chatham House – Journal of Cyber Policy CSIS – Cybersecurity and Technology research and publications CSIS – Global Cyber Strategies Index CSIS – Inside Cyber Diplomacy podcast series CYRILLA Collaboration – CYRILLA Global Digital Rights Law database Diplo, GIP – Digital Watch observatory EUISS, GMF, SMV – EU Cyber Direct Knowledge Hub EUISS, GMF, SMV – EU Cyber Direct's Cyber Diplomacy in the European Union GCSCC Oxford University – Cyber Security Capacity Maturity Model for Nations (CMM) GFCE – Cybil Portal GFCE, AU, EU, OAS – Global Cyber Expertise Magazine Government of Australia – Cyber Affairs and Foreign Policy webinar series ICT4Peace – Cybersecurity High-Level Policy Briefings ITU – Global Cybersecurity Index ITU – Guide to developing a national cybersecurity strategy - Strategic engagement in cybersecurity ITU – National Cybersecurity Strategies Repository	Choices randomised for each respondent

No.	Question	Notes
	Leiden University – Hague Program for Cyber Norms research and publications NATO CCDCOE – Cyber Defence Library NATO CCDCOE – Cyber Law Toolkit NATO CCDCOE – INCYDER NATO CCDCOE – Strategy and Governance NATO CCDCOE – Tallinn Manual NUPI – Centre for Digitalisation and Cyber Security Studies research and publications OCSC – Cybersecurity Capacity Maturity Model for Nations (CMM) UNIDIR – Cyber Policy Portal UNIDIR – International Cyber Operations research paper series I use other tools and/or resources, which are: No, I do not use any tools or resources	> Skip logic, Q15
14	**How often do you use these tools and resources?** [Date range]	Each tool, including respondent's listed tools, from Q13, is listed for each response
15	**Which best describes your reason(s) for not using the tools and resources listed in the survey, or any other tools and resources for your work in cyber diplomacy? (Tick as many as applicable)** I was not aware of them. I would like to start exploring them, as they might help me in my work. I would like to use them, but they are too difficult or complicated to use. I do not need to use any external tools or resources, as I have access to in-house tools and resources. I do not have time to use any tools or resources. I do not need to use any tools or resources. There were other reasons, including:	
16	**If you would like to receive the full list of cyber diplomacy training and tools as a result of our study, enter your email address.**	
17	**If you prefer to remain anonymous, we will do our best to disseminate the study as widely as possible. Please share any final comments below.**	

Annex II

Code	Acronym	Stakeholder	Title	Type	Descriptor	Modules or topics
Tr1	ADFA at Univ. of NSW	Academia	Master of Cyber Security, Strategy and Diplomacy	Online Master's programme	The programme provides an advanced interdisciplinary study into the political, military, diplomatic and higher level management aspects of issues where cyber security, strategy and diplomacy interact. This degree provides students with the ability to understand the main policy, operational, ethical and informational challenges for security resulting from the integration or penetration of advanced information technologies into all spheres of human activity.	Core credits: §1. Cybersecurity and world politics (key issues in cyber politics such as cyber espionage, information warfare, the risk of 'cyber war', the threats of corporate surveillance, and the struggle to economically dominate the internet; the strategies of the major players including the USA, Russia, China and the EU as they compete to assert dominance and control over this new domain); §2. Australian cyber diplomacy (the information economy as a foundation for national welfare and security; privacy and personal security in cyberspace; strategies for national security in cyberspace; Australian diplomacy on these issues); §3. Australia and cyber war (the cyber space revolution in military affairs; middle powers and their military cyber strategy; the politics of transformational change in the Australian Defence Force; national security innovation priorities; and proposals for an Australian cyber militia); §4. Cyber policy in China (development of cyber policy in China across social, economic, political, military and technological domains); §5. Cyberspace, national security, and law (the current state of the 'law' – both international and domestic – as it relates to cyber as a military and security capability).
Tr2	Norwich Univ.	Academia	Cyber Diplomacy	Online course (part of a Master's programme)	This course provides students the opportunity to synthesise learning from previous seminars and apply the concepts and principles by providing a practical or theoretical solution to challenges or issues of contemporary international importance and relevance in cyber diplomacy.	Practical and theoretical solutions to challenges or issues of contemporary international importance and relevance in cyber diplomacy (based on participant's choice of project).
Tr3	Clingendael	Civil society/think tanks	Clingendael Cyber Course	Online tailored workshop	The tailor-made workshop typically tackles issues related to cyberspace which diplomats are facing, including: How can diplomats effectively navigate in cyberspace? How should new challenges in cyberspace be addressed? And what is the role of diplomats when their nation faces emerging cyber threats?	Topics typically include: §1. The cyber risk landscape; how cyberspace and international relations interact; §2. Responding to international cyber incidents (using the Clingendael cyber toolbox); §3. The challenges of attribution; §4. Cyber norms, confidence building measures, and capacity building in cyber governance.
Tr4	Diplo	Civil society/think tanks	Cybersecurity Diplomacy	Online course	This course debates current critical topics, such as those addressed in the final report of the UN Cyber OEWG.	§1. The modules explain the strategic impact of cyber(in)security on the political, social and economic environment; analyse landmark cases, such as the SolarWinds hack; §2. tackle the cybersecurity issues on the diplomatic agenda and their impact on geopolitics (applicability of international law, norms and confidence building measures; particular concerns like protection of critical infrastructure and the supply chain, exploitation of vulnerabilities and the proliferation of malicious tools, challenges of attribution, etc; broader contexts like Internet governance, human rights and economic development); §3. discuss the roles that stakeholder should play for cyber-stability: states (and various national institutions, parliamentarians, etc), companies (and in particular the producers of digital products), incident responders (like CERT/CSIRT teams), the technical community, non-government organisations and advocacy groups, academia and the research community; §4. map multilateral processes (UN cyber GGE and OEWG, etc.) and multistakeholder processes (Paris Call for Trust and Security in Cyberspace, Tech Accord, Charter of Trust, and Geneva Dialogue on Responsible Behaviour in Cyberspace, etc.) that shape global cybersecurity agenda, work of regional organisations (ASEAN, OSCE, OAS, AU, SCO, etc.), and related discussions in other international and multilateral organisations and processes (UN Digital Cooperation, ITU, WTO, and SDGs process, etc.); §5. tackle the specificities of diplomatic and political processes, and identifying steps to prepare an institution to take part in those processes (capacity building, diplomatic skills, developing foreign policy, etc.).

Code	Proc.	Risks	IL	Norms	CBMs	CB	R&I	Cont.	Methodology	Target participants	Target country	Max. #	Cost	Fin. support	LINK	Duration	Academic
Tr1	x	x	x	x	x	x	x	x	Participants can elect to exit the programme at certificate stage, and can take each credit as a standalone online course.	Postgraduate scholars and practitioners in defence, justice, public safety, regulatory, management and information sciences.	Australia; global	UNK	AUS$39,120 for international students	Yes (such as assistance from Commonwealth)		1 year FT	Yes
Tr2	x	x	x	x	x	x	x	x	Participants research and prepare a written capstone project, that is, a paper suitable for publication in a professional or an academic journal. Course assignments maximize the exchange of student suggestions and comments on the various stages of the project.	Anyone	Global	UNK	UNK	UNK		6 hours	Yes
Tr3									The intensive training involves discussions, and uses the Clingendael Cyber Toolbox	National	Global	UNK	UNK	UNK		4 days	No
Tr4	x	x	x	x	x	x	x		The methodology of this hands-on course includes group readings, fireside chats with policy experts, and other interactive learning techniques	Diplomats, business and civil society delegates for digital policy and governmental relations, decision-makers, executives, and leaders from various sectors	Global	25	€800	Yes		5 weeks, 3-4 hours per week	No

Code	Acronym	Stakeholder	Title	Type	Descriptor	Modules or topics
Tr5	Diplo	Civil society/think tanks	Cybersecurity	Online course (part of a Master's programme)	This course covers technological and geopolitical risks, policy challenges, actors, and initiatives related to cybersecurity, especially those related to cybercrime, violence, child protection, the security of core infrastructure, and cyberwarfare. It also covers a broader context: the relations of cybersecurity with economic development and human rights.	§1. Introduction to security discusses the historical development of cybersecurity, and global and geostrategic challenges. §2. Cybersecurity risks focuses on the vulnerabilities of cyberspace as well as emerging threat actors, procedures, and tools. §3. Cybercrime defines and classifies cybercrime and analyses its economic and social impact, taking into account emerging technological and societal trends. §4. Violence and child protection provides a look at the ways terrorists abuse cyberspace, the challenges of violent extremism, and the topic of child safety. §5. Critical infrastructure and resources looks at the security and protection of critical infrastructure, including the Internet infrastructure, water supply facilities, transport, industrial facilities, and power plants. §6. Cyber conflicts and international security looks at the main risks for conducting warfare by cyber means. It then reviews challenges of the applicability of international law to cyberspace, as well as ongoing diplomatic efforts to define norms and confidence-building measures related to state behaviour in cyberspace. §7. Cybersecurity policy frameworks analyses national cybersecurity mechanisms, starting with examples of national cybersecurity strategies, followed by a close look at the importance, role, and structure of national computer emergency response teams (CERTs) and computer security incident response teams (CSIRTs). §8. Broader context of cybersecurity correlates cybersecurity and other social and political issues related to digital policies and Internet governance.
Tr6	GCSP	Civil society/think tanks	Meeting the Cyber Security Challenge – A Virtual Learning Journey	Online course	The course helps organisations, institutions, and governments examine social and political responses to cybersecurity challenges in conjunction with technical solutions. Participants learn to understand how technical and non-technical aspects of cybersecurity connect with each other. The course can be (has been) tailored to regions.	§1. What is cybersecurity? A socio-political perspective; §2. Technical foundations of cybersecurity; §3. Legal and political principles of cybersecurity; §4. Cybercrime; §5. Cyber defence; §6. Societal impacts of cybersecurity.
Tr7	GDF	Civil society/think tanks	Digital Diplomacy	Online course	The course follows the latest trends for diplomatic education, and trains beyond the use of social media to develop and implement strategies with tangible impact on the delivery of their objectives. The course introduces and enhances participants' understanding of the main fields of Digital Diplomacy thus providing them with competitive edge and necessary foundations to effectively navigate in cyberspace.	§1. Digital and cyber diplomacy (Overview; diplomacy as a form of institutionalised communication representation; exploring digital diplomacy through emergence, actors, definitions, and practice; digital Diplomacy, soft power, and virtual enlargement; diplomatic crisis communication, including practice, impact, and digital capabilities); §2. Artificial intelligence and diplomacy (Conceptualising AI; diplomacy and AI); §3. Cybersecurity (Cyber security 101, including cyber-threats (cyber-incidents, -crime, -warfare), technologies and systems, people, organisations, states, and cybersecurity, and simulating a cyber incident; Cyber policy and cyber diplomacy, including national cybersecurity strategies, UN norms and values, confidence building measures, sovereignty and strategic autonomy in the digital age, lessons and challenges for the development of global norms and CBMs; Capita selecta, including ethics, cybersecurity markets, and future perspectives); §4. The shifting world order in the digital age (Geopolitics, politics, economies, and society).

Code	Proc.	Risks	IL	Norms	CBMs	CB	R&I	Cont.	Methodology	Target participants	Target country	Max. #	Cost	Fin. support	LINK	Duration	Academic
Tr5	x	x	x	x	x	x	x	x	The highly interactive course is based on in-depth practitioner-led discussions, and includes weekly chat sessions, assignments, and other interactive elements.	Decision-makers and policy-shapers from various sectors	Global	25	€690 (certificate), €850 (accredited)	Yes		10 weeks	Yes
Tr6		x	x	x	x		x	x	The course includes a preparatory phase (2 weeks) for reflecting on own experience, engaging with preparatory content, and virtual introductions; followed by a synchronous sessions (3.5 days) for reading modules and participating in group discussions; followed by a final phase (6 days) for applying learning to individual context, a final group activity, and closing sessions. The course takes place on an interactive learning platform.	Government officials (including diplomats, military officers, intelligence analysts), staff from international organisations, representatives from the non-profit sector, and private sector actors.	Global, regional versions	UNK	CHF750	Yes (fee reduction for alumni)		4 weeks	No
Tr7	x	x		x	x		x	x	All four modules contain the same structural elements, including content, learning objectives, lesson material (text, video, documents, and lexicon terms), assessment, and a discussion board. Every module features two live lectures, with the module leader and a guest lecturer.	Anyone	Global	UNK	£595	UNK		4 weeks	No

Code	Acronym	Stakeholder	Title	Type	Descriptor	Modules or topics
Tr8	ICT4Peace	Civil society/think tanks	Cybersecurity Policy & Diplomacy Workshops	Online workshop	The workshop offers awareness on issues of international cyber security by public officials and diplomats (international law and norms, CBMs and international; cooperation as outlined in the UN GGE Reports, by ASEAN, OSCE, AU, OAS etc.); preparation of staff for negotiations on cybersecurity in the context of the OEWG and UN GGE; feedback from the regions to the international cyber security dialogue and discourse; better mutual understanding of related concepts, norms and measures, strengthened and possibly institutionalised cooperation among participating countries; exchange of concerns, best practices, policies and institutional arrangements in the field of cyber security; a network of alumni, lecturers and experts familiar with the international cybersecurity challenges and processes and willing to support the goals of implementing and universally promoting inter alia the UN GGE guidance on norms and CBMs.	§1. Introduction to the international peace and security goals related to uses of ICTs; §2. Links between national and international cyber security efforts, processes and actors; §3. Introduction to international cyber security consultations and dialogues (UN GGE, UN OEWG, ASEAN, ARF, OSCE, AU, OAS, London Process etc.); §4. Applicability of the international law as outlined in the UN GGE reports; §5. Norms of responsible state behavior as outlined in the UN GGE reports; §6. CBMs and international cooperation in the cyberspace (as outlined in the UN GGE, OSCE, ARF etc. reports); §7. Best practices in national cybersecurity strategy building, policy development and legislation; §8. Best practices in CERT building and CERT-CERT cooperation; §9. Regional and national cybersecurity concerns, perspectives and policy options.
Tr9	Australia National Univ.	Government	Cyber (Digital) Bootcamp	(Online) workshop	The workshop provides practical expert advice and skills training to working-level government officials from ASEAN countries. The Cyber Bootcamps aim to build participants' knowledge and awareness across the full breath of cyber affairs issues – from the associated opportunities and threats of cyberspace and technology, to cyber policy and operations governance and decision-making. The programme is a flagship activity of Australia's Cyber and Critical Tech Cooperation Program.	Topics typically cover the full breath of cyber affairs issues, from the associated opportunities and threats of cyberspace and technology, to cyber policy and operations, governance, and decision-making.
Tr10	Estonian MFA	Government	Tallinn Winter School of Cyber Diplomacy	Online workshop	The workshop focuses on cyber stability and accompanying measures. It covers best practices of cyber norms implementation, the applicability of international law in cyberspace, and increasing resilience in the area of cyber security.	Topics typically include: §1. Overview of the cyber stability framework: Norms of responsible state behaviour, international law, confidence and capacity building measures; §2. Implementing norms of responsible state behaviour and the way forward with the UN First Committee cyber processes; §3. Cyber norms implementation in practice; §4. Applying international law in cyberspace; §5. Capacity building in cyber issues: expectations, requirements and donor coordination challenges; §6. Building the organisational and technical cyber resilience at national level.
Tr11	Marshall Center	Government	International Program on Cyber Security Studies (iPCSS)	Course, workshop, mentorship	The programme emphasises and teaches participants how to best make informed decisions on cyber policy, strategy and planning within the framework of whole-of-government cooperation and approaches. It helps participants appreciate the nature and magnitude of today's threats and develops a common understanding of the lexicon, best practices, and current cyber initiatives within the public and private sectors.	§1. Internet governance; §2. Cyber capacity building; §3. Privacy and security; §4. Combating terrorism and cybercrime; §5. Information sharing; §6. Cyber statecraft development; §7. Internet freedom; §8. Protection of Intellectual Property; §9. Public-private partnerships; §10. Cyber protection of critical infrastructure

Code	Proc.	Risks	IL	Norms	CBMs	CB	R&I	Cont.	Methodology	Target participants	Target country	Max. #	Cost	Fin. support	LINK	Duration	Academic
Tr8	x		x	x	x		x	x	Expert-led discussion, with space for exchange of best practices and concerns on cyber issues, presentations and panel discussions, and tailored table-top exercises.	Public officials and diplomats in capitals and country delegations	Regional (Latin America, Caribbean, Africa, etc)	35	UNK	UNK		5 days	No
Tr9	x	x	x	x	x	x	x	x	In the face-to-face version of this intensive programme held in Australia, participants engage in interactive workshops, exercise scenarios, industry site visits, and dialogues with Australian government agencies. As part of the programme, participants implement a project which responds to a cyber-challenge or opportunity relevant to their domestic roles that contributes to a cyber-resilient Indo-Pacific.	Working-level government officials	ASEAN countries	UNK	UNK	UNK		Half day sessions	No
Tr10	x		x	x	x	x		x	The workshop includes panel discussions and case studies for participants, with the option of viewing the broadcast and asking questions during the livestream. The recording is available for anyone to watch, via Youtube and Facebook.	Anyone	Global	NA	NA	NA		2 days	No
Tr11		x				x	x	x	A programme includes opportunities for participants to network and establish contacts with other cyber-focused professionals.	Serving senior officials responsible for developing or influencing cyber legislation, policies, or practices, including diplomats, legislators, ministerial staffs, policy-makers, military and law enforcement officers, and other officials involved in cybersecurity serving throughout the whole-of-government.	USA	UNK	UNK	UNK		2 weeks	No

Code	Acronym	Stakeholder	Title	Type	Descriptor	Modules or topics
Tr12	Governments of AU, UK, CA, NL, and NZ with UNITAR	Government	Women and International Security in Cyberspace Fellowship	Online course, workshop, and mentorship	The training on multilateral negotiations, and workshop on UN cyber issues, are part of a fellowship programme which promotes greater participation by women in discussion at the United Nations (UN) on international security issues related to responsible state behaviour in cyberspace. The programme is a joint initiative of the governments of Australia, UK, Canada, the Netherlands, and New Zealand.	The programme trains fellows in multilateral negotiations, and on cyber issues relevant to international security in cyberspace.
Tr13	Goverments of AU, DN	Government	Cyber and Tech Retreat	Workshop (closed)	A workshop, in the format of a closed multistakeholder forum, provides a space for candid and constructive discussions on technology and foreign policy issues. A specialised vehicle for open engagement, the Cyber and Tech Retreat enables the building of meaningful working relationships where governments and industry are free to jointly understand the longer-term risks, opportunities and impacts of emerging technologies, and their impact upon foreign policy interests.	Topics typically include issues arising from the intersection of emerging technologies (such as AI and quantum computing) and international relations, including the increasingly profound impact of critical technologies on the foreign and security policy landscape.
Tr14	ESDC, national partners	Intergovernmental organisations	Cyberdiplomacy: A Tool for Strategic Security Policy	Residential workshop, preceded by an online course	This course, as part of a longer set of modules, presents the interaction between the main pillars of the EU cyber ecosystem and how these pillars interact and reinforce the global security stability by strengthening cyber resilience, building trust, and upscaling the cooperation among the global actors. It highlights the developments in the cyber external relations sphere, and equips participants with the knowledge to understand and implement capacity building measures, and to increase resilience and stability. During this module the participants will be able to understand the need to interact and be interoperable across the global cyber ecosystem, understand and identify the basic notions, actual challenges, to find ways to implement capacity building measures, increase the resilience and share some common views, but also understand how to apply EU's Cyber Diplomacy Toolbox.	§1. The EU cyber ecosystem (the rationale for cyber diplomacy; key concepts of cyber diplomacy; EU cyber ecosystem and the respective cyber domains; local/regional initiatives and trends in cyber diplomacy; global and EU cyberspace; EU organisations, agencies, and bodies involved in cyber diplomacy); §2. EU approach in bulding resilience and trust (EU cyber-related strategies and actions; policies, regulations, and directives related with cyber within EU; international cooperation; resilience building trough fighting against cybercrime, cyberdefence, and critical infrastructures protection); §3. The EU's model in external cyber capacity building (cyber governance in the EU and beyond; Cyber Diplomacy Toolbox; coordinated response to large-scale cybersecurity incidents and crises); §4. Countering hybrid threats through cyber diplomacy (existing and emerging threats; framework on hybrid threats, interaction with cyber).
Tr15	ESDC, national partners	Intergovernmental organisations	Cyber Security/ Defence Training Programme	Residential workshop, preceded by an online course	The course provides participants with an understanding of cybersecurity and defence aspects within the EU Common Security and Defence Policy (CSDP), and a detailed overview of cyber security action at EU level, and enhances participants' knowledge and skills to mitigate risks and threats in the cyber domain at an individual and organisational level. During the course, the formation of networks among individuals will be encouraged. The final goal of the course is to support the cyber-action within the EU institutions and EU member states.	§1. Awareness/basic level, including: history and development of CSDP; structures and procedures; EU global strategy, cybersecurity strategy and the cyber defence policy framework; cyber law, concepts, and policies; cyber security awareness, hygiene, forensic, risks and threats, mainstreaming in CSDP missions, and operations; §2. Advanced level, including cybersecurity objectives; strategic cyber threat and vulnerabilities assessment; EEAS and EC crisis response system, in particular in the cyber domain; cyber risk management in CSDP missions and operations; capability development, including research and technology; cybersecurity and the EU's integrated approach; §3. Operational planning, including operational risk management; cyber risk assessment in missions and operations; integration of cyber elements in the operational and mission planning process; CIS accreditation; implementation of cyber aspects for CSDP operations and missions; implementation of the Cyber Diplomacy Toolbox; §4 (Alumni conference) New developments in the cyber environment; strategies, laws, policies, and concepts; new risks and threats; regional and horizontal CSDP issues.

Code	Proc.	Risks	IL	Norms	CBMs	CB	R&I	Cont.	Methodology	Target participants	Target country	Max. #	Cost	Fin. support	LINK	Duration	Academic
Tr12	x	x	x	x	x	x	x		A course, and a workshop, as well as mentoring events matching fellows with senior colleagues currently working on cyber issues at the UN in New York, and participation in OEWG meetings in NY.	Early to mid-career female diplomats	ASEAN, Pacific, South America and Commonwealth countries	35	UNK	Yes (travel support)		UNK	No
Tr13		x					x	x	Discussions held in a private setting	Senior officials from governments, technology companies, and academia, by invitation	Global	UNK	UNK	UNK		1 day	No
Tr14	x	x				x	x	x	Residential workshop, preceded by an online course	Mid- to high-level diplomats and officials from government, EU institutions, and other state agencies with a role in strategy formulation and implementation in the cyber realm.	EU member states and EU institutions, including agencies	UNK	UNK	UNK		Approx. 4 days (including online course)	Yes
Tr15		x	x			x	x	x	Residential workshop, preceded by an online course	Government officials with limited or no experience of cyber security/cyber defence.	EU member states and EU institutions, including agencies	UNK	UNK	UNK		Approx. 2 weeks (including online course)	Yes

Code	Acronym	Stakeholder	Title	Type	Descriptor	Modules or topics
Tr16	ESDC, national partners	Intergovernmental organisations	The EU's Cybersecurity Strategy for the Digital Decade	Residential workshop, preceded by an online course	This course presents the main pillars of the EU's Cybersecurity Strategy for the Digital Decade. It will act as a forum for where entities coming from EU member states, institutions, and agencies can interact with the participants and inform them on the current and future developments at strategic, tactical and operational levels regarding the EU's Cybersecurity Strategy. Furthermore, this course will allow the participants to exchange their views and share best practices on related topics of the Strategy by improving their knowledge, skills and competencies and better align with the overall objectives of the Strategy.	§1. Stability in the Global Environment (analysis of the impact of the cyber security in the global stability); §2. The EU's cybersecurity strategy for the digital decade (objective of the strategy; the EU cyber ecosystem); §3. Resilience, technological sovereignty, and leadership (resilient infrastructure and critical service; building a European cyber shield; an ultra-secure communication infrastructure; securing the next generation of broadband mobile networks; an internet of secure things; greater global internet security; a reinforced presence on the technology supply chain; a cyber-skilled EU workforce); §4. Building operational capacity to prevent, deter, and respond (CSIRTs community; tackling cybercrime; EU Cyber Diplomacy Toolbox; boosting cyber defence capabilities; a Joint Cyber Unit); §5. Advancing a global and open cyberspace (EU leadership on standards, norms, and frameworks in cyberspace, including standardisation, international security, crime, and human rights; cooperation with partners and the multistakeholder community; strengthening global capacities to increase global resilience); §6. The EU approach in hybrid threats (the conceptual framework on hybrid threats and the interaction with cyber).
Tr17	ESDC, national partners	Intergovernmental organisations	The Role of the EU Cyber Ecosystem in the Global Cyber Security Stability	Residential workshop, preceded by an online course	This course presents the main pillars of the EU cyber ecosystem and how these pillars can reinforce the global security stability by strengthening the cyber resilience, build trust, and upscaling the cooperation among the global actors. It will allow participants to exchange their views and share best practices on cyber-related topics by improving their knowledge, skills and competencies.	§1. The EU cyber ecosystem (EU agencies and bodies with cyber-related tasks); §2. The EU approach to building resilience in cyberspace (policies, regulations, and directives related to cyber within the EU); §3. The EU's external cyber capacity building (Joint Communication on 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU'); §4. The EU approach to hybrid threats (conceptual framework and the interaction with cyber); §5. Stability in the global environment (analysis of the impact of the cybersecurity on global stability).
Tr18	ESDC, national partners	Intergovernmental organisations	Challenges of European Cyber Security	Residential workshop, preceded by an online course	The course enables participants to understand the extensive nature of the information society and to recognise its complexity and the different threats, as well as the basic notions and concepts related to cyber security and cyber defence, as well the international cyber space issues and the cyber diplomacy. Offering an overview on technological tools used in the cyber security and cyber defence, the course aims at providing an opportunity to create a network of people working in the field.	§1. Cyber space and cyber strategy (overall contextual framework: past, present and future trends; definitions and concepts of cybersecurity; trends in cyber threats and critical infrastructures; towards a strategic autonomy for EU in cyber-space; European cybersecurity strategy; EU's implementation of cybersecurity national cyber-security policies; cybersecurity on private infra-structure); §2. Cybersecurity and cyber defence (the EU and CSDP's needs; critical infrastructure protection against cyber attacks; assessment and perspectives of EU's progress in cybersecurity; policy frameworks, directives, and capacities); Cyber war and cybercrime (legal framework for cyber operations; UN Charter and international humanitarian law in cyberspace; promoting the Budapest Convention; cyber regulation in the EU and national best practices; digital combat in the conduct of military operations; specificity of military cyberspace; incidence of digitisation and robotisation of the battlefield; cross-domain warfare); Cyber diplomacy and cyber co-operation (preventing cyber war and the role of confidence building measures, the EU's role in reinforcing member states' capacities; actions of EDA; human resource capacity building; building a European cyber industry; cyber diplomacy and international cyber issues; intelligence, interference, and cyber diplomacy).
Tr19	ENISA	Intergovernmental organisations	ENISA National Cyber Security Strategies (NCSS) workshop	Online workshop (by invitation)	The annual workshop is one of the ways in which ENISA supports the efforts of EU member states in providing guidelines on how to develop, implement, and update NCSS, analyse existing strategies and outline good practices.	Typical topics include: §1. Development, implementation and evaluation of national cybersecurity strategies (NCSSs); §2. Information Sharing and Analysis Centres (ISACs) and public-private co-operation; §3. Assessment frameworks to examine a country's maturity level in cybersecurity capabilities.

Code	Proc.	Risks	IL	Norms	CBMs	CB	R&I	Cont.	Methodology	Target participants	Target country	Max. #	Cost	Fin. support	LINK	Duration	Academic
Tr16		x		x			x	x	Residential workshop, preceded by an online course	Officials dealing with aspects in the field of cybersecurity	EU member states and EU institutions, including agencies	UNK	UNK	UNK		Approx. 4 days (including online course)	Yes
Tr17						x	x	x	Residential workshop, preceded by an online course	Mid-ranking to senior officials dealing with aspects in the field of cybersecurity	Non-EU countries	UNK	UNK	UNK		Approx. 4 days (including online course)	Yes
Tr18	x	x	x	x	x	x	x	x	Residential workshop, preceded by an online course	Mid-ranking to senior officials dealing with strategic aspects in the field of cybersecurity and cyber defence, who are either working in key positions or have a clear potential to achieve leadership positions in the field.	EU member states and EU institutions, including agencies	UNK	UNK	UNK		Approx. 4 days (including online course)	Yes
Tr19							x	x	An online workshop, by invitation only	Practitioners involved in the development, implementation, and evaluation of national cybersecurity strategies (NCSS) and people involved in ISACs, including national policy and decisionmakers, legislators, regulators, and national authorities, private sector, and academia.	EU member states	UNK	UNK	UNK		1 day	No

Code	Acronym	Stakeholder	Title	Type	Descriptor	Modules or topics
Tr20	NATO CCDCOE	Intergovernmental organisations	Executive Cyber Seminar	Online workshop	The workshop offers an introduction to and basic, but comprehensive, grounding in cyberspace; what it is, and what it is not; why cyberspace is important and relevant to decision makers and those who write policy and strategy; introduction to the legal aspects of cyberspace operations; and a perspective of the threat landscape.	§1. Introduction of the domain of cyberspace; its impact on societies and decision makers; why cyberspace is important and relevant to decision-makers and those who write policy and strategy; §2. Introduction to the legal aspects, including a review on how International Law applies to cyber operations; §3. A perspective of the threat landscape in and through cyberspace; §4. Other topics, including NATO and EU developments, critical information infrastructure protection, the role of social media etc.
Tr21	NATO CCDCOE	Intergovernmental organisations	International Law of Cyber Operations	Online or f2f workshop	This course provides a practice-oriented survey of the international law applicable to cyber operations involving States that occur both in peacetime and in the context of an armed conflict.	§1. Peacetime international law governing cyber operations, including issues on sovereignty, jurisdiction, due diligence, the law of state responsibility, the prohibition of intervention and self-defence, all in the cyberspace operations context. It will answer questions such as which cyber operations outside an armed conflict violate international law, when can states hack back, and when has a cyber armed attack occurred such that states may engage in self-defence. §2. International humanitarian law that applies during armed conflict involving cyber operations, including traditional international humanitarian law topics such as classification of cyber conflict, the principle of distinction during cyber operations, and targetable and protected persons and objects in the cyber context. §3. Overview of the technical aspects of Internet structure and of defensive and offensive cyber operations.
Tr22	OSCE	Intergovernmental organisations	Cyber/ICT security Confidence-Building Measures Course	Online course	This course provides an overview of OSCE's work in the field of cyber/ICT security. Participants learn why and how confidence-building measures play and important role in promoting international security of and in the use of ICTs.	§1. Introduction into the international world of ICTs. With a brief overview of the work of the United Nations, it will describe the four pillars of the international framework for stability in cyberspace and discuss the role of regional organizations, like the OSCE, in these efforts. §2. The development of cyber/ICT security in the OSCE and the 16 Confidence-Building Measures the Organization's participating States have adopted. §3. A closer look at each of the 16 cyber CBMs individually, with a specific focus on practical implementation.
Tr23	SELA	Intergovernmental organisations	Specialization Course on Cyber Diplomacy	Online workshop	The workshop looks at the relationship between diplomacy and technology, and examines the application of diplomacy to the political and geopolitical problems arising in cyberspace. It helps participants acquire and develop technical capabilities that will be useful in the treatment of the issues on the global agenda. The aims are: to train participants in the analysis of regulatory challenges and future agendas on the regularization of cyberspace; to ensure that public officials in the study area have the knowledge and skills to negotiate in an international cyber community, which are not exempt from inter-state and relations conflicts; to exchange information and experiences on the use of cyber diplomacy in the international agenda; and to assess the future implications of cyber diplomacy on the foreign policy agendas of the countries of the Latin American and Caribbean.	§1. Introduction to cyber diplomacy (A matter of definitions: Cyber diplomacy, digital diplomacy and e-diplomacy; the application of diplomacy to solve the problems generated in cyberspace; the geopolitics of cyberspace); §2. Internet governance (The conflict between agendas: Internet governance vs cybersecurity; free internet nations vs cyber-sovereignty advocates; ICANN vs ITU; key issues of Internet governance); §3. Cybersecurity (Different types of cyberattacks; geopolitical and criminal motivations; the cybersecurity dilemma; diplomacy and cybersecurity); §4. International law in cyberspace (The law of armed conflict in cyberspace; building standards of behaviour in cyberspace; multistakeholder diplomacy).

Code	Proc.	Risks	IL	Norms	CBMs	CB	R&I	Cont.	Methodology	Target participants	Target country	Max. #	Cost	Fin. support	LINK	Duration	Academic
Tr20	x	x	x				x	x	Themed discussions	Senior level military and civilian staff, primarily those in NATO and defence, and government officials with policy or decision making responsibility	CCDCOE member nations	UNK	€500	Yes (1 free slot per CCDCOE member nation and NATO bodies)		1.5 days	No
Tr21	x	x	x	x			x	x	Practice-oriented sessions, concluding with a complex exercise that allows participants to apply the law addressed during lectures and discussion. The session on jus in bellum is taught from an operational legal advisor's perspective.	Military and civilian legal advisors to the armed forces, Intelligence community lawyers, Other civilian attorneys in the government agencies responsible for security issues, Policy specialists who advise on cyber issues and wish to acquire a basic understanding of the applicable legal regimes, Legal scholars and graduate students	CCDCOE member nations	UNK	€500	Yes (1 free slot per CCDCOE member nation and NATO bodies)		5 days	No
Tr22	x				x		x		A self-paced course featuring readings, video recordings, quizzes, and a learning scenario.	Anyone	Global	NA	Free	NA		1 day	No
Tr23	x	x	x	x			x	x	The training is divided into four online workshops, and includes teaching material in both written and multimedia format. The training is offered in Spanish, with a translation into English (if necessary)	Diplomatic public officials and international negotiators	Latin America and the Caribbean	60	UNK	UNK		4 days, 2 hours each session, for a total of 8 hours	No

Code	Acronym	Stakeholder	Title	Type	Descriptor	Modules or topics
Tr24	INCIBE, OAS	Intergovernmental organisations	Cybersecurity Summer Boot Camp	Online workshops	The annual training programme specialises in cybersecurity, and provides participants with practical knowledge. The programme aims to increase the cybersecurity capabilities of participants and encourage the development of a global network of cybersecurity experts.	General topics, and topics in the LEA and policymakers' track, include: §1. The cybersecurity regulatory framework in various regions; §2. Cybersecurity risks and challenges; §3. International law applicable to cyber operations; §4. Digital forensics; §5. National cybersecurity strategies; §6. Cybercrime and emerging technologies, such as cryptocurrencies.
Tr25	UNIDIR, UNODA	Intergovernmental organisations	Disarmament Orientation Course	Online course	This online orientation course for Geneva disarmament diplomats is designed and presented jointly by UNIDIR and UNODA. The module on ICT, Cyber, and LAWS, provide an overview of the implications for international security and arms control of current and emerging information and AI technologies, and helps participants understand the roles and operations of the multilateral processes established to address these issues.	§1. Scene-setting: context, history and mechanisms; §2. Weapons of mass destruction; §3. Cross cutting disarmament issues: Gender, the humanitarian perspective, and financing aspects (including the relationship between international humanitarian law and disarmament; the role of IHL in creating and implementing disarmament and arms control treaties); §4. Conventional weapons; §5. Space and missiles; §6. ICT, Cyber, and LAWS, including, artificial intelligence (AI) and machine learning (ML) (military applications of AI/ML; AI/ML implications for verification of disarmament, arms control and non-proliferation regimes); cyber issues and the two UN processes addressing international security and the use of information and communication technologies: the Open-Ended Working Group and the Group of Governmental Experts; lethal autonomous weapons systems (LAWS) including the CCW Group of Governmental Experts on LAWS.
Tr26	UNITAR	Intergovernmental organisations	Digital and Cyber Diplomacy	Online course	The course equips participants with the practical skills to make the best use of digital tools in pursuing diplomatic objective. It will also help them understand better the challenges and difficulties digital technologies pose for diplomacy. At the same time, it will help them better understand the broad range of problems being generated in cyberspace and how diplomacy can be applied to managing them. It will help learners make the best use of digital tools in promoting diplomatic objectives, and develop effective strategies for managing the multiple problems thrown up by the growing cyberspace.	§1. Digital Diplomacy (A question of definition; political analysis and consular protection; public diplomacy and social media; algorithms and beyond social media; and digital technologies, diplomats and foreign ministries); §2. Cyber diplomacy (Diplomacy and the problems of cyberspace; Internet governance; cybersecurity and cyber diplomacy; diplomacy and cybercrime; and the diplomat in cyberspace).
Tr27	UNITAR	Intergovernmental organisations	International Humanitarian Law and Cyber Warfare	Online workshop	This workshop forms part of (second session) the International Law in Focus Series. During the three-part e-workshop, participants explore methods and means of cyber warfare, and learn to distinguish between the applicability of international humanitarian law to cyber operations in international armed conflicts and non-international armed conflicts.	§1. Introduction to Humanitarian Law and Cyber Operations; §2. Cyber Warfare; §3. Cyber Operations and Human Rights. §4. The workshop includes an introduction to the Cyber Policy Portal.
Tr28	UNODA	Intergovernmental organisations	Online Cyberdiplomacy Training Course	Online course	This course enhances the understanding, particularly of the 2013 and 2015 GGE reports by addressing the five pillars of the GGE reports: existing and emerging threats; how international law applies to the use of ICTs; norms, rules and principles for the responsible behaviour of States; confidence-building measures; and international cooperation and assistance in ICT security and capacity-building.	§1. Introduction to the GGE process. What is the GGE process and how does it work? What issues have the GGEs considered? §2. Existing and emerging threats. What threats to international ICT security have been identified by the GGEs? What foreseeable developments could exacerbate existing threats? §3. International law. How does international law apply to the use of ICTs? What recommendations have the GGEs made in this area? §4. Norms, rules and principles. What are the 11 voluntary, non-binding norms of responsible State behaviour recommended by the GGEs? §5. Confidence-building measures. What are confidence-building measures and why do we need them with respect to ICTs? What are the key GGE recommendations for confidence-building? What CBM initiatives already exist? §6. International cooperation and assistance in capacity-building. How can States work together to build their capacity to further the peaceful use of ICTs? How can we ensure sustainability in capacity-building?

Code	Proc.	Risks	IL	Norms	CBMs	CB	R&I	Cont.	Methodology	Target participants	Target country	Max. #	Cost	Fin. support	LINK	Duration	Academic
Tr24		x	x				x	x	The programme consists of two master classes open to the public, and 18 hours of training over 6 sessions of technical workshops restricted to the selected students.	Policymakers, law enforcement agencies, public prosecutors, judges and magistrates, and Cyber Incident Response Centre specialists.	Global	UNK	NA	UNK		8 days	No
Tr25	x	x	x				x	x	The course consists of six thematic modules, with each module comprising a reading list, an introductory video and a 120-minute interactive online videoconference session.	Geneva disarmament diplomats	Global	UNK	UNK	UNK		4 days	No
Tr26	x	x					x	x	An asynchronous course, which places emphasis on online discussions and self-paced learning. The participants are responsible for their own learning over the four-week span of the course. The course consists of the following components: compulsory and optional reading material, intended to teach the basic concepts and principles of the lesson's subject-matter; external links to additional books, articles, documents, and websites related to the lessons; and quizzes and case studies at the end of each module. A Community Discussion Board is available participants to post questions or comments visible to the instructor and other participants, which is moderated by the course director and UNITAR. A simulation exercise is included.	The course targets junior to senior-level governmental officials as well as staff of intergovernmental and nongovernmental organizations. It also targets entry-level and mid-career diplomats and private and public sector specialists. Postgraduate students with relevant experience in multicultural working environment are also encouraged to apply.	Global	UNK	$600	UNK		3-4 weeks	No
Tr27		x	x	x				x	The three-part workshop is conducted online on Zoom, from 1 pm to 5 pm Geneva time. The material presented in the workshop is interactive; the workshops include assignments.	The International Law in Focus series is aimed at students and professionals seeking a deeper understanding of international law.	Global	UNK	$650	Yes (participants form SIDS and LDCs; low and middle income countries; LDCs)		3 days	No
Tr28	x	x	x	x	x	x			A self-paced course featuring animated audio-visual learning methods, complemented by interactive elements, including quiz questions, exercises and other elements that encourage the participant to apply their newly acquired knowledge. Interviews by experts provide different perspectives. Every module ends with a recap. Additional resources offered throughout the course are compiled for the user's reference and further studying.	Anyone	Global	NA	Free	NA		7 sessions of 0.5 to 1 hour each session	No

Annex III

Code	Provider	Acronym	Stakeholder	Name of initiative	Type	Descriptor	Beneficiary country	URL
TI1	Centre of Excellence for National Security (CENS), S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore	CENS Singapore	Academia	Publications on Cybersecurity	Research and publications	The centre's mission is to raise the intellectual capital invested in strategising national security. To achieve this mission, the research and publications by CENS Singapore feature policy-relevant analysis across a range of national security issues.	Global	
TI2	ETH Zurich	ETHZ	Academia	Cyber Security Politics Publications	Research and publications	This resource on cybersecurity politics is curated by ETH Zurch's Center for Security Studies, and gathers publications written by CSS staff, or articles on cybersecurity politics featuring commentary by CSS staff.	Global	
TI3	Global Cyber Security Capacity Centre at the University of Oxford	GCSCC Oxford University	Academia	Global Cybersecurity Capacity Maturity Model for Nations (CMM)	Toolkit guidelines and manuals	The Cybersecurity Capacity Maturity Model for Nations (CMM) is a methodical framework designed to review a country's cybersecurity capacity. The CMM considers cybersecurity to comprise five Dimensions which, together, constitute the breadth of national capacity that a country requires to be effective in delivering cybersecurity: Developing cybersecurity policy and strategy; encouraging responsible cybersecurity culture within society; building cybersecurity knowledge and capabilities; creating effective legal and regulatory frameworks; and controlling risks through standards and technologies.	Global	
TI4	Leiden University	Leiden University	Academia	Hague Program for Cyber Norms: Research and publications	Research and publications	The research published by the Hague Program for Cyber Norms contributes to the international debate on cyber norms. The Hague Program focuses on the development and implementation of cyber norms, and asks how norms are and can be applied to support cyber security, stability and peace. For this purpose, it examines how consensus is developing, among governments, academics and the society, on certain norms and how they should apply to state behaviour in cyberspace. It also investigates the development of normative thought and scholarship in this field and contributes to the dialogue about standards of responsible behaviour in use of ICTs.	Global	
TI5	UC Berkeley Center for Long-Term Cybersecurity	CLTC at UC Berkeley	Academia	The Internet Atlas	Online databases and indices	The Internet Atlas measures long-term structural risks to the global Internet, to identify points of strength and weakness at various levels of the Internet 'stack'. Measurement is a key policy tool: As central banks watch measures of inflation and employment as they decide how to set monetary policy, internet governance should rely on independent and reproducible indicators to guide and structure decision-making.	Global	
TI10	Center for Strategic and International Studies	CSIS	Civil society/think tanks	Inside Cyber Diplomacy	Research and publications	This series of podcasts presents a wide-ranging and thought-provoking look at international cybersecurity, its challenges, and practices. Through candid interviews with experts around the world, co-hosts Jim Lewis and Chris Painter explore how diplomacy and negotiation have shaped the field. The series is supported by the Cyber Security Agency of Singapore and the Estonian Ministry of Foreign Affairs.	Global	

Code	Provider	Acronym	Stakeholder	Name of initiative	Type	Descriptor	Beneficiary country	URL
TI11	Center for Strategic and International Studies	CSIS	Civil society/think tanks	Significant Cyber Incidents	Online databases and indices	This timeline records significant cyber incidents since 2006 with focus on cyber attacks on government agencies, defense and high tech companies, or economic crimes with losses of more than a million dollars.	Global	
TI12	Center for Strategic and International Studies	CSIS	Civil society/think tanks	Cybersecurity and Technology	Research and publications	This set of research and publications looks at how rapidly changing technology and cybersecurity are affecting the world in the 21st century. Issues covered include intelligence, surveillance, encryption, privacy, military technology, and space.	Global	
TI13	Center for Strategic and International Studies	CSIS	Civil society/think tanks	Global Cyber Strategies Index	Online databases and indices	The database provides an index of existing cyber strategies and laws by country and territory, which includes national strategies addressing civilian and military national cyber defense, digital content, data privacy, critical infrastructure protection, e-commerce, and cybercrime. This provides policymakers and diplomatic officials a unified, at-a-glance database of global legal and policy frameworks to help the global community understand, track, and harmonise regulations internationally.	Global	
TI14	Chatham House	Chatham House	Civil society/think tanks	Journal of Cyber Policy	Research and publications	The Journal is a peer-reviewed resource for emerging issues in cyber policy. Topics include cyber crime, internet governance and emerging technologies. It is published three times a year.	Global	
TI15	Chatham House	Chatham House	Civil society/think tanks	International Security Programme	Research and publications	This resource includes research and other publications on the impact of emerging technologies, conflict prevention, and international obligations on security policies worldwide.	Global	
TI16	Council on Foreign Relations	CFR	Civil society/think tanks	Cyber Operations Tracker	Online databases and indices	The Digital and Cyberspace Policy programme's cyber operations tracker is a database of the publicly known state-sponsored incidents that have occurred since 2005	Global	
TI17	Council on Foreign Relations	CFR	Civil society/think tanks	Cybersecurity; Net Politics	Research and publications	CFR experts investigate the impact of information and communication technologies on security, privacy, and international affairs.	Global	
TI18	Cyberscurity Capacity Centre for South Africa	C3SA	Civil society/think tanks	Cybersecurity Capacity Maturity Model for African nations (CMM)	Toolkit guidelines and manuals	The work of C3SA is anchored in the deployment of the Cybersecurity Capacity Maturity Model for African nations (CMM) in countries throughout Southern African and where opportunities arise, the broader Sub-Saharan Africa region. C3SA identifies and collaborates with local, regional, and international partners to complete CMM reviews and ensure the results of the assessments enable decision-makers in governments and partners to identify cybersecurity gaps and focus on priority areas for capacity building investments and policy development.	South Africa	
TI19	CYRILLA Collaborative	CYRILLA Collaboration	Civil society/think tanks	CYRILLA: Global Digital Rights Law	Online databases and indices	CYRILLA is an open database of digital rights law from around the world. The multilingual database is developed and maintained by the CYRILLA Collaborative, a global initiative that seeks to map and analyse the evolution and impacts of legal frameworks on digital environments, particularly in the Global South. The database includes legislation, cases, and analyses concerning human rights in digitally-networked spaces.	Global	

Code	Provider	Acronym	Stakeholder	Name of initiative	Type	Descriptor	Beneficiary country	URL
TI20	DiploFoundation, Geneva Internet Platform	Diplo, GIP	Civil society/think tanks	Digital Watch observatory	Online databases and indices	This is a comprehensive digital policy observatory, which provides a neutral one-stop shop for the latest developments, overviews, events, actors, instruments, and other resources. The observatory is part of the Geneva Internet Platform, an initiative of the Swiss authorities, operated by DiploFoundation.	Global	
TI21	DiploFoundation/ Microsoft	Diplo	Civil society/think tanks	Cyberconflict	Research and publications	This resource gathers research, publications, and webinar summaries on issues related to cyberconflict. It includes the summaries of the cyber diplomacy series of web discussions.	Global	
TI22	EU Institute for Security Studies (EUISS), German Marshall Fund of the United States (GMF), Stiftung Neue Verantwortung (SNV)	EUISS, GMF, SMV	Civil society/think tanks	EU Cyber Direct Knowledge Hub	Online databases and indices	The EU Cyber Direct's Knowledge Hub as a 'one-stop-shop' which includes: Research and analysis delivered as part of the EU Cyber Direct project; updates about cyber-related policies and legal developments in the EU and partner countries; and research and analysis on cyber-related policies in the EU and partner countries and regions.	Global	
TI23	Global Partners Digital	GPD	Civil society/think tanks	Multistakeholder Approaches to National Cybersecurity Strategy Development	Toolkit guidelines and manuals	Drawing on GPD's own research into multistakeholder processes, as well as real life examples of good practice in Chile, Ghana, Kenya, and Mexico, this resource sets out clear guidelines and recommendations for multistakeholder approaches to NCSS development that can be employed in a range of contexts.	Global	
TI24	ICT4Peace	ICT4Peace	Civil society/think tanks	Cybersecurity High-Level Policy Briefings	Research and publications	The resource includes high-level briefings on cybersecurity.	Global	
TI25	Institute for Security + Technology	IST	Civil society/think tanks	Virtual Library	Online databases and indices	This repository which gathers open-source resources on security and technology which showcase research and analysis that has directly influenced the work of the IST.	Global	
TI26	Just Security	Just Security	Civil society/think tanks	Cyber	Research and publications	This resource gathers analysis of national and international security which aims to promote principled and pragmatic solutions to problems confronting decision-makers in the USA and beyond.	Global	
TI27	Lawfare Blog	Lawfare	Civil society/think tanks	Library on Cybersecurity	Research and publications	This resource is a collection of articles which focus on the merits of the underlying legal and policy debates themselves – the 'Hard National Security Choices'.	Global	
TI28	National Cyber Security Index	NCSI	Civil society/think tanks	National Cyber Security Index	Online databases and indices	This global index measures the preparedness of countries to prevent cyber threats and manage cyber incidents. The NCSI is also a database with publicly available evidence materials and a tool for national cybersecurity capacity building.	Global	
TI29	Norwegian Institute of International Affairs	NUPI	Civil society/think tanks	NUPI's Centre for Digitalization and Cyber Security Studies	Research and publications	NUPI's Centre for Digitalization and Cyber Security Studies seeks to bridge the gap between the technical community and the policy world with research focusing primarily on the political dimension of cybersecurity. With a focus on the role of cybersecurity in international relations, the centre tracks new developments in cybersecurity, and provides academic studies, expert analysis, and strategic policy recommendations. The research focus includes theories of cybersecurity, global governance of cyberspace, capacity building, development, and the security vs freedom dilemma.	Global	

Code	Provider	Acronym	Stakeholder	Name of initiative	Type	Descriptor	Beneficiary country	URL
TI30	Oceania Cyber Security Centre	OCSC	Civil society/think tanks	Cybersecurity Capacity Maturity Model for Nations (CMM)	Toolkit guidelines and manuals	This tool provides complimentary national cybersecurity reviews to nations in the Pacific using the Cybersecurity Capacity Maturity Model for Nations (CMM). The tool is used by OCSC and the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford to review national cybersecurity capacity and conduct related research in the Pacific. The OCSC team travels to the host nation to meet with a variety of stakeholders across sectors, building up a comprehensive understanding of national cybersecurity capacity informed by the people involved in it, to focus on what is important for the nation in context ensuring that the CMM recommendations are relevant and applicable.	Pacific	
TI31	ORF America (formerly led by the EastWest Institute)	ORF America	Civil society/think tanks	Cyberspace Cooperation Initiative	Research and publications	The research and publications in this collection aim to promote dialogue on the current challenges to security and stability in cyberspace. Since 2009, the Cyberspace Cooperation Initiative - then with the EastWest Institute - initiated some of the earliest dialogue on the critical issues of cooperation in cyberspace and organised Global Cyber Coopertion Summits.	Global	
TI32	Potomac Institute for Policy Studies	Potomac Institute for Policy Studies	Civil society/think tanks	Cyber Readiness Index	Online databases and indices	The Cyber Readiness Index evaluates and measure a country's preparedness levels for certain cybersecurity risks. The team of experts apply the CRI to provide a compelling and actionable review of a country's policies, plans, laws, standards, market levers (e.g., incentives and regulations), and other initiatives.	Global	
TI33	The Global Commission on the Stability of Cyberspace	GCSC	Civil society/think tanks	Cyberstability Paper Series	Research and publications	This resource gathers research papers, published by the Global Commission, on the challenges and contributions to cyberstability. The papers are released on a rolling basis from July until December 2021, culminating in an edited volume.	Global	
TI6	Atlantic Council		Civil society/think tanks	Cyber Statecraft Initiative: In-Depth Research & Reports	Research and publications	This collection of articles, issue briefs, and reports consist of notes from the field and analysis from the Atlantic Council's Scowcroft Center for Strategy and Security team, on the complex challenges of cybersecurity.		
TI7	Brookings Institution	Brookings	Civil society/think tanks	Cybersecurity	Research and publications	This resource includes research, publications, and multimedia content on cybersecurity.	Global	
TI8	Carnegie Endowment for International Peace	Carnegie Endowment for International Peace	Civil society/think tanks	Cyber Norms Index	Online databases and indices	The resource tracks and compares the most important milestones in the negotiation and development of norms for state behaviour in and through cyberspace.	Global	
TI9	Carnegie Endowment for International Peace	Carnegie Endowment for International Peace	Civil society/think tanks	Cyber Resilience and Financial Organizations: A Capacity-building Tool Box	Toolkit guidelines and manuals	This resource offers a series of action-oriented, easy-to-use one-page guides, complementary checklists, and a comprehensive, supplementary report detailing how financial institutions, particularly small- and mid-sized organisations as well as those that are less cyber mature, can enhance their own security as well as that of their customers and third parties. The guides and checklists are available in multiple languages (Arabic, Dutch, English, French, Portuguese, Russian, and Spanish).	Global	
TI34	Council of Europe	Council of Europe	Intergovernmental organisations	Octopus Cybercrime Community Country Wiki	Online databases and indices	The resource provides an overview of a country's policy on cybercrime and electronic evidence. Every fiche includes a description of cybercrime policies/strategies, the state of cybercrime legislation, the channels of cooperation, international cooperation, and case law.	Global	

Code	Provider	Acronym	Stakeholder	Name of initiative	Type	Descriptor	Beneficiary country	URL
TI35	EU Agency for Cybersecurity	ENISA	Intergovernmental organisations	National Cyber Security Strategies of EU member states	Online databases and indices	The ENISA NCSS Interactive Map lists all the documents of national cybersecurity strategies in the EU together with their strategic objectives and good examples of implementation. ENISA's goal is to create an info-hub with information provided by the member states on their efforts to enhance national cybersecurity.	Global	
TI36	EU Agency for Cybersecurity	ENISA	Intergovernmental organisations	National Cybersecurity Strategies: Publications	Toolkit guidelines and manuals	This is a collection of toolkits and guidelines on building national cybersecurity capabilities, and on responding to other cybersecurity challenges.	Global	
TI37	EU Agency for Cybersecurity	ENISA	Intergovernmental organisations	National Capabilities Assessment Framework	Toolkit guidelines and manuals	This report presents the work performed by ENISA to build a National Capabilities Assessment Framework (NCAF). The framework aims at providing Member States with a self-assessment of their level of maturity by assessing their NCSS objectives, that will help them enhance and build cybersecurity capabilities both at strategic and at operational level. This framework was designed with the support of ENISA subject matter experts and representatives from 19 Member States and EFTA countries. The target audience of this report is policymakers, experts and government officials responsible for or involved in designing, implementing and evaluating an NCSS and, on a broader level, cybersecurity capabilities.	Global	
TI38	Global Forum on Cyber Expertise	GFCE	Intergovernmental organisations	Cybil Portal	Online databases and indices	Cybil is a knowledge sharing portal for the international cyber capacity building community, facilitated by the Global Forum on Cyber Expertise (GFCE). It is a place where governments, funders and implementing agencies can find and share best practices and practical information to support the design and delivery of capacity building projects and activities. Cybil also acts as a source of information on cyber security and cybercrime capacity building for civil society, academia and the technical community, in line with the GFCE's commitment to transparency and inclusion	Global	
TI39	Global Forum on Cyber Expertise with African Union, the European Union, Organization of American States	GFCE, AU, EU, OAS	Intergovernmental organisations	Global Cyber Expertise Magazine	Research and publications	The Global Cyber Expertise Magazine is a bi-annual magazine on global cyber policy developments and capacity building projects. The Magazine is jointly published by the African Union, the European Union, the Global Forum on Cyber Expertise and the Organization of American States.	Global	
TI40	International Telecommunication Union	ITU	Intergovernmental organisations	National Cybersecurity Strategies Repository	Online databases and indices	This repository includes national cybersecurity strategies, including single and multiple documents, and documents forming an integral part of a broader ICT or national security strategies.	Global	

Code	Provider	Acronym	Stakeholder	Name of initiative	Type	Descriptor	Beneficiary country	URL
TI41	International Telecommunication Union	ITU	Intergovernmental organisations	Guide to developing a national cybersecurity strategy - Strategic engagement in cybersecurity	Toolkit guidelines and manuals	The guide's aim is to instigate strategic thinking and help national leaders and policymakers to develop, establish, and implement national cybersecurity strategies worldwide. In the guide, facilitated by ITU, 12 partners from the public and private sectors, academia and civil society share their experience, knowledge and expertise, providing an aggregated, harmonised set of principles on the development, establishment, and implementation of national cybersecurity strategies.	Global	
TI42	International Telecommunication Union	ITU	Intergovernmental organisations	Global Cybersecurity Index	Online databases and indices	The Global Cybersecurity Index (GCI) measures the commitment of countries to cybersecurity at a global level – to raise awareness of the importance and different dimensions of the issue. As cybersecurity has a broad field of application, cutting across many industries and various sectors, each country's level of development or engagement is assessed along five pillars – (i) Legal Measures, (ii) Technical Measures, (iii) Organizational Measures, (iv) Capacity Development, and (v) Cooperation – and then aggregated into an overall score.	Global	
TI43	International Telecommunication Union	ITU	Intergovernmental organisations	Global Cybersecurity Index (GCI) v4	Online databases and indices	The Global Cybersecurity Index (GCI) measures the commitment of countries to cybersecurity at a global level – to raise awareness of the importance and different dimensions of the issue. As cybersecurity has a broad field of application, cutting across many industries and various sectors, each country's level of development or engagement is assessed along five pillars – (i) Legal Measures, (ii) Technical Measures, (iii) Organizational Measures, (iv) Capacity Building, and (v) Cooperation – and then aggregated into an overall score.	Global	
TI44	Organization of American States	OAS	Intergovernmental organisations	Cybersecurity Awareness Campaign Toolkit	Toolkit guidelines and manuals	This toolkit is designed to provide governments or organisations guidance and resources for developing a cybersecurity awareness campaign, with the goal to help think through a country's needs for a cybersecurity awareness campaign and how to best achieve it.	Global	
TI45	Organization of American States with the Inter-American Development Bank	OAS/IDB	Intergovernmental organisations	Observatory Cybersecurity in Latin America and the Caribbean	Online databases and indices	The observatory provides an overview of the state of cybersecurity in Latin America and Caribbean countries, with the aim of providing guidance on strengthening national cybersecurity capacities.	Global	
TI46	The NATO Cooperative Cyber Defence Centre of Excellence	NATO CCDCOE	Intergovernmental organisations	Strategy and Governance	Online databases and indices	This is a comprehensive overview of national cybersecurity organisations in NATO countries, together with a selection of national cybersecurity policy and legal documents adopted by NATO Allies and like-minded partners beyond the Alliance.	Global	
TI47	The NATO Cooperative Cyber Defence Centre of Excellence	NATO CCDCOE	Intergovernmental organisations	Cyber Defence Library	Online databases and indices	This is database of publications authored or co-authored by CCDCOE researchers and experts, visiting researchers and other partners.	Global	
TI48	The NATO Cooperative Cyber Defence Centre of Excellence	NATO CCDCOE	Intergovernmental organisations	Cyber Law Toolkit	Toolkit guidelines and manuals	This is an interactive toolkit consisting of hypothetical scenarios of cyber incidents inspired by real-world examples, and a detailed analysis to examine the applicability of international law to the scenarios and the issues they raise. The resource is aimed at legal professionals who work with matters at the intersection of international law and cyber operations, and may be explored and utilised in different ways.	Global	

Code	Provider	Acronym	Stakeholder	Name of initiative	Type	Descriptor	Beneficiary country	URL
TI49	The NATO Cooperative Cyber Defence Centre of Excellence	NATO CCDCOE	Intergovernmental organisations	Tallinn Manual	Toolkit guidelines and manuals	The Tallinn Manual is the flagship research initiative of the CCDCOE. The original Tallinn Manual (published in 2013 by Cambridge University Press) addressed the most severe cyber operations – those that violate the prohibition of the use of force, entitle states to exercise their right of self-defence, or occur during armed conflict. The Tallinn Manual 2.0, published in 2017, built on that work by considering the rules of international law governing cyber incidents that states encounter on a day-to-day basis but which fall below the thresholds of the use of force or armed conflict. Emerging State practice and the taking of public positions on international cyber law many States since the Manual's publication necessitated an update of the 2017 edition. Accordingly, in 2021, the CCDCOE launched the Tallinn Manual 3.0 Project, a five-year initiative that will involve the revision of existing chapters and the exploration of new topics of importance to states.	Global	
TI50	The NATO Cooperative Cyber Defence Centre of Excellence	NATO CCDCOE	Intergovernmental organisations	INCYDER	Online databases and indices	This interactive database features the most relevant cybersecurity documents from major international organisations and articles by CCDCOE researchers on recent trends and developments within these organisations.	Global	
TI51	United Nations Institute for Disarnament Research	UNIDIR	Intergovernmental organisations	UNIDIR Cyber Policy Portal	Online databases and indices	This is an online reference tool that maps the cybersecurity and cybersecurity-related policy landscape. Through concise and comprehensive profiles, it provides a rigorous, accessible and up-to-date overview of the cyber capacity of UN Member States and a select group of intergovernmental organisations.	Global	
TI52	United Nations Institute for Disarnament Research	UNIDIR	Intergovernmental organisations	International Cyber Operations: National Doctrines and Capabilities Research Paper Series	Research and publications	The research papers outline national capabilities to conduct international cyber operations and relevant national doctrines regulating the conduct of such operations. They were commissioned by the UNIDIR Security and Technology Programme to facilitate transparency, advance trust among states and thus promote stability in international cyberspace. In the resulting papers, nine scholars and practitioners provide an overview of capabilities and doctrines pertaining to 15 countries across different regions: Australia, Brazil, Canada, China, France, Germany, India, Iran, Israel, Japan, the Republic of Korea, Russia, Saudi Arabia, the UK, and the USA.	Global	
TI53	United Nations Office on Drugs and Crime	UNODC	Intergovernmental organisations	UNODC Cybercrime Repository	Online databases and indices	The cybercrime repository is a central data repository of cybercrime laws and lessons learned for the purposes of facilitating the continued assessment of needs and criminal justice capabilities and the delivery and coordination of technical assistance.	Global	

Code	Provider	Acronym	Stakeholder	Name of initiative	Type	Descriptor	Beneficiary country	URL
TI54	United Nations/World Bank	UN/World Bank	Intergovernmental organisations	Combatting Cybercrime: Tools and Capacity Building for Emerging Economies	Toolkit guidelines and manuals	The resources available as part the World Bank's Combatting Cybercrime initiative are aimed at building capacity among policymakers, legislators, public prosecutors, investigators, and civil society in developing countries in the policy, legal and criminal justice aspects of the enabling environment to combat cybercrime. There are three main resources: A toolkit that synthesises good international practice in combatting cybercrime; an assessment tool that enables countries to assess their current capacity to combat cybercrime and identify capacity-building priorities; and a virtual library with materials provided by project participating organisations and others.	Global	
TI55	World Economic Forum Centre for Cybersecurity	WEF C4C	International organisations	Reports	Research and publications	This resource gathers reports on cybersecurity by the World Economic Forum's Center for Cybersecurity.	Global	

Global Affairs Canada

Affaires mondiales Canada