CARIBBEAN TELECOMMUNICATIONS UNION

4 Mary Street, St. Clair, Port of Spain, Trinidad and Tobago
Tel:(868) 628-0281,628-6359,622-5871 Fax:(868) 622-6523 E-Mail: info@ctu.int URL: www.ctu.int

13th April 2021

Dear Permanent Secretaries and Technical Officers,

Application for scholarships to attend a course on
Cybersecurity Diplomacy – Commencing 17th May 2021

The Caribbean Telecommunications Union (CTU) is inviting you to nominate public officers to apply for scholarships to attend a course on Cybersecurity Diplomacy, which is being offered as a joint venture between the CTU and DiploFoundation and which will be hosted virtually for the duration of **five (5) weeks commencing 17th May 2021**.

The Cybersecurity Diplomacy course complements a longer and more intensive suite of academic cybersecurity courses and will be the first in a series of online training courses offered by the DiploFoundation to CTU Member States in digital policy and diplomacy. The partnership between CTU and DiploFoundation will see the delivery of a series of online workshops, focusing on internet governance and other emerging technology issues, including research of topics such as artificial intelligence, big data, science diplomacy, and cybersecurity.

The CTU and DiploFoundation share a common philosophy and vision to improve the role of small and developing states in global diplomacy, by presenting national leaders and policy makers with concepts to enable a greater reach into larger systems of which they and their organisations are a part. Our shared goal is to resource small and developing Caribbean states by building capacity to engage effectively in international policy processes, negotiations and diplomacy.

The overall objectives are to develop the capacity of policy makers in the Caribbean by:

- Raising understanding of digital policy issues and processes;
- Preparing delegates to meaningfully participate in global and regional negotiations;
- Shaping and advancing Caribbean positions on digital policy.

The Cybersecurity Diplomacy course is specifically intended to equip participants with the knowledge and skills they need to act effectively in cybersecurity diplomacy. This online course analyses how the abuse of technology impacts geopolitical security, social and economic development, and cyber processes and negotiations. The course is taught by academics, technology experts, and seasoned diplomats.

Nominated scholarship applicants are invited to complete the registration for the Cybersecurity Diplomacy course at: Cybersecurity diplomacy.

I look forward to receiving applications and the active participation of public officers in the Cybersecurity Diplomacy training course.

(https://www.diplomacy.edu/)

Home (/) / Cybersecurity Diplomacy

Cybersecurity Diplomacy

> *The Cybersecurity Diplomacy course equips professionals with the knowledge and skills they need to act effectively in cybersecurity diplomacy. This online course analyses how the abuse of technology impacts geopolitical security, social and economic development, and cyber processes and negotiations. The course is taught by academics, technology experts, and seasoned diplomats.*

Notice how **cybersecurity** news has moved from 'lifestyle' and 'tech' sections to '**politics**', and even '**breaking news**'?

The increasingly frequent and high-impact **cyber breaches**, **hacks**, and **attacks** are **influencing global political and economic relations**, and pushing states to the negotiating table. From the UN General Assembly and Security Council, to the G7, G20, the WTO, and various regional organisations like the AUC, OSCE, OAS and ASEAN, states are forced to find ways to secure cyberspace. Cyber(in)security is impacting international peace, sustainable development, digital cooperation, human rights and privacy, as well as the global digital business environment, and stakes are getting higher for everyone: ministers, diplomats, business executives, civil society leaders, tech gurus, and top researchers.

All this confronts us with a number of interesting and crucial challenges, that we cover in this cybersecurity training:

- **Can international diplomacy**, together with regional and national policies, **address technology-related threats** in current geopolitical contexts?
- How can diplomats, businesses and civil society leaders **promote collaboration over confrontation**?

- How can we ensure that **agreements** on secure behaviour in cyberspace can **preserve the internet's potential** for universal access, economic and social development, and individual security, rights, and freedoms?
- **How can YOU prepare yourself and your institution** to take an active part in these processes?

Interested in becoming actively involved in cybersecurity negotiations and processes that aim to make our global cyberspace a safer place?

Diplo's Cybersecurity Diplomacy course **debates current critical topics**, such as those addressed in the final report of the UN Cyber OEWG, through **group readings, fireside chats with policy experts**, and other **interactive learning** techniques.

With Diplo's well-recognised, engaging, and interactive learning methodology, this cybersecurity training provides a space for **exchanging experiences and views within s select group of professionals** from around the world, as well as with lecturers who are among the top professionals and senior diplomats active in cybersecurity.

Join this practically oriented and intellectually inspiring course by registering from the form above.

This Cybersecurity Diplomacy course complements our longer and more intensive academic Cybersecurity course (https://www.diplomacy.edu/courses/cybersecurity), which provides a much broader overview of cybersecurity policy, including combating cybercrime and terrorism, protecting critical infrastructure, national policies and international cooperation, and the interplay between cybersecurity, economic development and human rights.

To learn more about the two main UN cybersecurity processes (GGE and OEWG), visit our Digital Watch observatory (https://dig.watch/processes/un-gge).

Interested in how the security aspects of digital technology shape geopolitics - international peace and stability, and social and economic development? Do you want to learn how to contribute to various processes that shape the global cybersecurity environment? Then this online cybersecurity course is for you.

Diplo's Cybersecurity Diplomacy course is for 'hands-on' practitioners such as:

- Diplomats
- Business and civil society delegates for digital policy and governmental relations
- Decision makers, executives, and leaders from various sectors

You don't need to be a tech or policy expert to attend the course. All technical, legal, diplomatic, and policy aspects will be explained in this cybersecurity training in a clear, easier to understand, and appealing manner. The unique value of the course lies in the exchange of experiences and knowledge within a network of professionals from various backgrounds, as well as a well-crafted learning approach designed and facilitated by seasoned diplomats and experts.

The knowledge, insights, and contacts gained in this course are applicable in: deliberations of international and regional organisations, government policy decisions, strategic planning and governance relations for businesses, academic research and education, civil society advocacy work, and raising public awareness via media.

Scope

Understanding the geopolitical aspects of cybersecurity and preparing for influencing and taking part in the global negotiations and processes.

Learning objectives

By the end of this cybersecurity diplomacy course you should be able to:

- Explain the impact of (in)security of digital technologies on geopolitics and social and economic development;
- Understand cybersecurity issues on the diplomatic agenda and their impact on geopolitics;
- Identify multilateral and multistakeholder political processes that shape global and regional cybersecurity agendas;
- Explain the roles that stakeholder (states, companies, emergency responders, civil society, and academia) should play in achieving cyber-stability;
- Identify steps to prepare an institution to take part in those processes;
- Take an active role in international processes around strategic digital/cyber policy.

Guest lecturers

The course will involve number of guest lecturers, among others:

Ambassador Jürg Lauber (https://www.eda.admin.ch/dam/mission-onu-omc-aele-geneve/en/documents/Jurg-Lauber-CV-Sep-2020_EN.pdf), former Chair of the UN Open-Ended Working Group (OEWG) on Developments in the Field of ICTs in the Context of International Security, and Permanent Representative of Switzerland to the United Nations and other Organizations in Geneva

Ambassador Amr Aljowaily (https://www.diplomacy.edu/people/aljowaily), former Vice Chair of the UN Disarmament Commission and Rapporteur of the United Nations' Special Committee on Peacekeeping, and Ambassador of Egypt to Serbia

Mr Ljupčo Jivan Gjorgjinski (https://www.diplomacy.edu/people/gjorgjinski), former Chair of the UN Group of Governmental Experts (GGE) on lethal autonomous weapons systems (LAWS), and Senior Advisor for Multilateral Affairs at the MFA of North Macedonia

Mr Chris Painter (https://thegfce.org/foundation_board/chris-painter/), former Coordinator for Cyber Issues at the US Department of State, President of the GFCE Foundation

Course outline

- Explaining the strategic impact of cyber(in)security on the political, social and economic environment. Analysis of landmark cases, such as the SolarWinds hack.
- Understanding 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).
- Discussing 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.
- Mapping 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.).
- Understanding 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.).

DiploFoundation