

COURSE SYLLABUS

Diplomacy 4.0 – Beyond the Digital Frontier

e-learning | 27 April - 7 June, 2020



Table of Contents

Table of Contents.....	2
Disclaimer and Acknowledgements	3
Course Presentation	4
Course Outline and Contents.....	5
Learning Objectives	9
Methodology	11
Grading Policy and Course Completion	15
Study Planning.....	16
Learning Content	17
1. Interactive Course	17
2. Cybrary	17
Experts.....	11
Technical Support	20

Disclaimer and Acknowledgements

Please carefully read the Disclaimer and Acknowledgements documents located on this course's home page before beginning the course for more information about the terms and conditions of use of UNITAR's virtual learning environment and acknowledgement of those organizations for their authorization to use audio transcripts, webcasts and photographic imagery.

Course Presentation

The last couple of decades have seen an unprecedented expansion and absorption of Information Technology not only in virtually all industries but also (and arguably most importantly) in our everyday lives. Regardless of this ever-increasing pace of development and role of digital communication diplomats and Ministries of Foreign Affairs have sometimes be reluctant to adapt new tools and techniques into diplomatic practice.

As a result, the diplomatic practices and procedures have not kept up with the growth of not only contemporary digital communication methods but also with the emergence of social media platforms, therefore creating a knowledge and skills vacuum. Likewise, the rapidly increasing capability of using Information Technology for offensive purposes forms an uncharted territory for present and future diplomats and international civil servants. Though still in its infancy the impact of the Artificial Intelligence on our world is already being discussed. While current discussions focus mainly on the economic and social aspects of this phenomenon it is also important to initiate debate on the influence AI may have on international relations and multilateralism.

Technology was always one of the main driving forces behind the development of human kind and shaping of the world that we live in. Never before however the changes introduced by technological progress were so rapid and so wide-spread – new technologies are available almost simultaneously across the globe and virtually everyone can access them. The same can be said about the access to information – human kind has never had such a wide and easy access to data.

In such circumstances diplomats and governments can no longer afford to stay behind. The United Nations Institute for Training and Research (UNITAR) has developed the e-Learning Course in Diplomacy 4.0 to introduce and enhance participants' understanding of the main fields comprising for the Diplomacy 4.0 thus providing them with competitive edge and necessary foundations to effectively navigate in Cyberspace.

Course Outline and Contents

Module 1: The Neoteric Diplomat (27 April - 3 May 2020)

Lesson 1: Defining Diplomacy 4.0

- 1.1 Sustaining vs disruptive innovation
- 1.2 Digital technologies as drivers of change

Lesson 2: Interconnectedness of Diplomacy 4.0 pillars

- 2.1 Representation (digital diplomacy)
- 2.2 Communication (cybersecurity)
- 2.3 Negotiation (AI)

Lesson 3: Neoteric Diplomat – a practitioner of Diplomacy 4.0

- 3.1 Adaptive leadership
- 3.2 Strategy vs tactics
- 3.3 Trends and Counter-Trends

Estimated learning time: 8 – 10 hours

**Module 2: Digital and Cyber Diplomacy
(4 - 10 May 2020)****Lesson 1: A Question of Definition and Political Reporting**

- 1.1 Introduction
- 1.2 Diplomacy and Diplomats
- 1.3 Confusion of Terminology
- 1.4 Digital Tools
- 1.5 Areas of Diplomatic Activity
- 1.6 Digital Diplomacy and Information Gathering
- 1.7 Analysing the Information
- 1.8 Big Data
- 1.9 Consular Protection

Lesson 2: Public Diplomacy and Social Media

- 2.1 Public Diplomacy
- 2.2 Social Media Tools
- 2.3 The Dangers of Social Media
- 2.4 The Problems of Algorithms: Social Media
- 2.5 The Problems of Algorithms: Search Engines
- 2.6 Alternative Digital Tools
- 2.7 Gamification

Lesson 3: Cyberdiplomacy and Internet Governance

- 3.1 Cyberdiplomacy
- 3.2 Problems in Cyberspace
- 3.3 International Institutions and International Law
- 3.4 Internet Governance: Key Issues
- 3.5 21st Century Regulation and Multi-Stakeholder Diplomacy

Lesson 4: Cybersecurity and Cyberdiplomacy

- 4.1 Cybersecurity
- 4.2 The Cybersecurity Dilemma
- 4.3 Diplomacy and Cybersecurity

Lesson 5: The Diplomat in Cyberspace

- 5.1 The Impact of Digital Technologies on Diplomats
- 5.2 The Impact of Digital Technologies on Foreign Ministries
- 5.3 Hybrid Diplomacy
- 5.4 Diplomatic strategy in Cyberspace
- 5.5 The Tech Ambassador

Estimated learning time: 8 – 10 hours

Module 3: Cybersecurity (11 - 17 May 2020)

Lesson 1: Introduction to Cyber Security for Diplomats

- 1.1. History
 - 1.1.1 History of the Internet
 - 1.1.2 History of Cyber threats
 - 1.1.3 Current Cyber Threats
- 1.2. Threats & Defense Context Introduction
 - 1.2.1 Cyber threats Actors
 - 1.2.2 Cyber Kill Chain Explained
 - 1.2.3 Attack Vectors
 - 1.2.4 Technologies, Processes, People

Lesson 2: Cyber Warfare

- 2.1. Digital Complexification
 - 2.1.1 A New Frontier
 - 2.1.2 Malware-Industrial Complex
 - 2.1.3 Malware Arms Race Deterrence Concept
- 2.2. Cyber-Geopolitics
 - 2.2.1 Cyber-Strategies and International Laws
 - 2.2.2 Traditional Geopolitics vs Cyber Geopolitics
 - 2.2.3 Information Operations, Fake News and Post Truth Era

Lesson 3: Good Practices for Diplomats Regarding Cybersecurity

- 3.1 Contextualization
- 3.1 CIA Triad & Defense Technics: Technologies, Processes, People
- 3.1 Information Gathering
- 3.1 Social Engineering (By Email, by Phone)
- 3.1 Physical Attacks
- 3.1 Network Attacks
- 3.1 Smartphones
- 3.1 Best Practices on Travel

Lesson 4: OSINT (Refresh Lesson Based on OSINT Training)

- 4.1 Introduction to OSINT
- 4.2 Anonymity (technical part and user part)
- 4.3 Methodology of research
- 4.4 Divers research (emails, images, phone numbers, website, etc.)
- 4.5 Social Media (geopolitics at stake)
- 4.6 Dark web

Estimated learning time: 8 – 10 hours

Module 4: Artificial Intelligence (18 - 24 May 2020)

Lesson 1: Definitions and origins

- 1.1 AI, AGI, Machine Learning and Neural Networks
- 1.2 Big Data Analytics

Lesson 2: Regulating development of AI and global governance

- 2.1 Agile governance – global initiatives
- 2.2 AI policies - Standards and principles
- 2.3 Data Commons

Lesson 3: Ethics and Trust in AI

- 3.1 Black box dilemma
- 3.2 Accountability and explainability

Lesson 4: Autonomous weapons and new threat

- 4.1 Digital social engineering – impact on society

Lesson 5: Beyond narrow AI

Estimated learning time: 8 – 10 hours

Module 5: Internet Governance (25 - 31 May 2020)

Lesson 1: Internet History, Principles & Governance

- 1.1: The evolution of Internet
- 1.2: Internet Design Principles
- 1.3: Introduction to Internet Governance

Lesson 2: Diplomacy & Internet Governance

- 2.1: National and Transnational Organisations' role in governing the internet
- 2.2: Private Sector – passive observer or active contributor?
- 2.3: Some of the Key Global Internet Governance Issues

Estimated learning time: 8 – 10 hours

Module 6: Science Diplomacy (1 - 7 June 2020)

Lesson 1: Science Diplomacy as a Holistic Process

- 1.1. Understanding our globally-interconnected civilization across centuries
- 1.2. Learning lessons of cold-war cooperation among the two superpowers
- 1.3. Balancing national and common interests with science as a tool of diplomacy

Lesson 2: Engine of Science Diplomacy (Methods and Theory of Informed Decision-making)

- 2.1. Researching with questions and data in view of systems
- 2.2. Integrating data into evidence with governance mechanisms
- 2.3. Acting with evidence and options (without advocacy) for decisions
- 2.4. Addressing issues, impacts and resources from security to sustainability time scales

Lesson 3: Engine of Science Diplomacy (Skills of Informed Decision-Making)

- 3.1. Capacity-building with holistic integration as both observer and participant
- 3.2. Transforming research and action for informed decision-making
- 3.3. Facilitating dialogues among allies and adversaries alike
- 3.4. Accelerating knowledge co-production
- 3.5. Common-interest building to promote cooperation and prevent conflict

Lesson 4: Science, Technology and Innovation (STI) Ecosystems

- 4.1. Connecting the natural and social sciences with Indigenous knowledge
- 4.2. Creating holistic capacities across networks
- 4.3. Operating from sub-national to international levels within urban centres
- 4.4. Developing knowledge economies
- 4.5. Achieving progress with sustainability at local-global scales

Lesson 5: Sustainable Development Goals (SDG) as a Gift for Humanity

- 5.1. Empowering inclusion from global-local scales
- 5.2. Balancing economic, environmental and societal perspectives in a holistic manner
- 5.3. Responding to change with informed decision-making for sustainability
- 5.4. Informed decision-making as the apex goal with lifelong learning
- 5.5. Applying SDG pedagogy to train next-generation science diplomats

Estimated learning time: 8 – 10 hours

Learning Objectives

Module	Learning objectives At the end of the module, you will be able to:
Module 1 (1 week) Neoteric Diplomat	<ul style="list-style-type: none"> ▪ Explain the difference between sustainable vs disruptive forms of technological innovation and relate that to the concept of Diplomacy 4.0 ▪ Understand the mechanisms by which technological innovations inform, shape and influence areas of Diplomacy 4.0 in terms of representation, communication, and negotiation ▪ Recognize the opportunities and challenges that the Neoteric Diplomat may face in terms of leadership, strategic action, and future (counter) trends of digital transformation

<p>Module 2 (1 week)</p> <p>Digital and Cyber Diplomacy</p>	<ul style="list-style-type: none"> ▪ Understand the range of diplomatic tools available to facilitate and promote different diplomatic activities; ▪ Understand the advantages and disadvantages of social media in public diplomacy strategies; ▪ Understand how digital tools can enhance the capacities and reach of smaller countries and non-state actors; ▪ Develop digital diplomacy strategies in pursuit of broader foreign policy objectives; ▪ Identify the key problems of internet governance and how diplomatic mindsets and techniques can be applied to managing them; ▪ Distinguish between the different aspects of cybersecurity and the challenge they pose to governments, companies and society; ▪ Understand the cybersecurity dilemma; ▪ Be able to apply diplomatic approaches to managing cybersecurity challenges.
<p>Module 3 (1 week)</p> <p>Cybersecurity</p>	<ul style="list-style-type: none"> ▪ Describe the history of the Internet, cyber threats, cyber actors and cyber-attacks; ▪ Understand how the cyberspace and geopolitics are intertwined and affect international relations; ▪ Be able to apply the best practices regarding cybersecurity in different situations of your daily private and professional lives; ▪ Perform more efficiently online research on the Internet.
<p>Module 4 (1 week)</p> <p>Artificial Intelligence</p>	<ul style="list-style-type: none"> ▪ Explain differences between AI and related concepts, such as Machine Learning, and AGI ▪ Explain the main use of AI technology and Big Data in various sectors and industries, including impact and implications on jobs, education, health etc. ▪ Understand the need for systemic thinking in a global context, including geopolitics of AI and Trust & Ethics in AI ▪ Differentiate between global governance and agile governance of AI ▪ Explain risks and opportunities on society of autonomous weapons and new threats of autonomous and intelligent systems

<p>Module 5 (1 week)</p> <p>Internet Governance</p>	<ul style="list-style-type: none"> ▪ Describe the origin and history of the Internet ▪ Identify key infrastructure elements and components that make up the internet ▪ Describe and discuss Internet Design Principles ▪ Understand the Relationship between Universal Human Rights and Internet Design Principles ▪ Define Internet Governance and Classify various types of Internet governance issues ▪ Utilize a conceptual framework for analyzing Internet-related issues ▪ Understand that a myriad of different actors have valid roles to play in Internet Governance - The Internet Ecosystem ▪ Appreciate the role of the Multi-stakeholder approach. ▪ Understand the role of private sector in promoting the growth of the internet ▪ Identify the role & need for regulations ▪ Appreciate and discuss the implications of contemporary Internet Governance Issues
<p>Module 6 (1 week)</p> <p>Science Diplomacy</p>	<ul style="list-style-type: none"> ▪ Understand the context of our globally-interconnected civilization across the 21st century; ▪ Contrast informed and un-informed decisions from diverse perspectives; ▪ Apply common-interest building as a negotiating strategy, starting with questions; and ▪ Contribute as a 'science diplomat' with balance for the benefit of all at local-global levels.

Experts



Prof. Corneliu Bjola

Module 1: Neoteric Diplomat

Corneliu Bjola is Associate Professor in Diplomatic Studies at the *University of Oxford* and Head of the [Oxford Digital Diplomacy Research Group](#). He also serves as a Faculty Fellow at the *Center on Public Diplomacy* at the *University of Southern California* and as a Professorial Lecturer at the *Diplomatic Academy of Vienna*. His research focuses on the impact of digital technology on the conduct of diplomacy with a focus on strategic communication, digital influence, data analytics and methods for countering digital propaganda.

He has authored or edited six books, including the twin volumes on *Countering Online Propaganda and Violent Extremism: The Dark Side of Digital Diplomacy* (2018) and *Digital Diplomacy: Theory and Practice* (2015). His work has been published in the *European Journal of International Relations*, *Review of International Studies*, *Ethics and International Affairs*, *International Negotiation*, *Cambridge Review of International Affairs*, *Global Policy*, *Journal of Global Ethics* and the *Hague Journal of Diplomacy*. @cbjola www.cbjola.com



Shaun Riordan

Module 2: Digital and Cyber Diplomacy

Mr. Shaun Riordan is a Senior Visiting Fellow of the Netherlands Institute for International Relations “Clingendael”, a member of the Social Media Team of The Hague Journal of Diplomacy, and a member of the Public Diplomacy Advisory Board of the Sustainable Development Goals Fund. He served 16 years as a British Diplomat, including postings to New York, Beijing and Madrid, and spells in the Counter-Terrorism and Eastern Adriatic Units of the Foreign Office. Since leaving the Diplomatic Service, he has worked as a consultant to both governments and companies on geopolitical risk and innovation in diplomacy. He lectures in Diplomatic Academies in Armenia, Spain, the Dominican Republic and Bulgaria. His publications include The

New Diplomacy (2003), Adios a la Diplomacia (2005) and Cyberdiplomacy: Doing Diplomacy in Cyberspace.



Kudelski Security

Module 3: Cybersecurity

Kudelski Security is an independent provider of tailored cybersecurity solutions to enterprises and public sector institutions, delivering workable solutions to the toughest security challenges they face.

As part of the Kudelski Group, Kudelski Security embodies the same innovative spirit that has inspired the company since its creation in 1951. Our innovation is purposeful; we strive to create and deliver cybersecurity solutions that answer real problems.

We help our clients in their journey to design, deploy, and manage effective cybersecurity through a combination of advisory services, technology deployments, managed security services, and custom research and development.

We build on the concrete expertise of the Kudelski Group and their creation of ground-breaking technology that has shaped the evolution of the digital content ecosystem. Together with the Group, we hold thousands of patents and apply the rich engineering expertise of 3,900+ employees worldwide to the solutions we create and deliver in the cybersecurity marketplace.

Our global reach and comprehensive cyber solutions focus are reinforced by key international partnerships. These include alliances with the world's leading security technology firms as well as with experts in specialized services, so clients have access to all the tools and talent they need in order to plan, deploy, and run effective cybersecurity programs.



Gosia Loj

Module 4: Artificial Intelligence

Currently an AI Policy Advisor to The Future Society, Gosia helped deliver the Global Governance of AI Round Table (GGAR) at the World Government Summit 2019 in Dubai as part of the executing team on behalf of the Minister

of AI, UAE where she chaired a sub-committee on decentralized approaches to AI global governance.

As the AI Global Governance Lead, Gosia established an AI Global Governance Commission in 2018 for the Secretariat of the UK All Party Parliamentary Group on AI to help shape future AI policy and regulations internationally and delivered the vision and strategy for implementation.

Between 2011 and 2017, Gosia worked with several international organisations and the United Nations' agencies, including the WTO, WIPO, NATO, and the European Commission both in Brussels, Belgium and Geneva, Switzerland in the field of international standards, strategies and regulations as well as results-based management. In 2016 she took up a role of a CEO for a greenNet Solutions start-up. She began her career in 2008 working for NGOs in Argentina and Brazil as well as PwC Chile.

She holds a BSc (Hons) in Politics with Economics from the University of Bath, UK, a MSc in International Development from the University of Amsterdam, Netherlands, and an Executive Program Certificate in Innovation and Technology from MIT, USA. Gosia speaks English, Polish and Spanish fluently, and has a working knowledge of Portuguese and French.



John Walubengo

Module 5: Internet Governance

Mr. Walubengo holds an MSc in Strategic Business IT (University of Portsmouth) and a BSc in Mathematics (Kenyatta University). He holds several industry certifications including the CCNA (Certified Cisco Network Associate) and the CISA (Certified Information Systems Auditor) certification. His area of specialisation is in ICT Governance, Security, Policy & Strategy.

He has over 20 years of experience in the ICT Training and Consulting. His work experience included working for the Strathmore University as the IT Course Director and as the founding Dean, Faculty of Computing at the Multimedia University. He is currently a PhD candidate at the University of Nairobi and continues to provide Consultancy services to Government and other organisations. Most recently, he was appointed a member of two critical Taskforces looking into emerging technologies and policies. These are the National TaskForce on Blockchain & Artificial Intelligence as well as the Data Protection Taskforce respectively. He also writes a [weekly column on topical ICT issues](#) in one of the largest dailies in East and Central Africa.



Prof. Paul Arthur Berkman

Module 6: Science Diplomacy

Professor Paul Arthur Berkman is a science diplomat, applying, training and refining informed decision-making to balance national interests and common interests for the benefit of all on Earth across generations. He became a Visiting Professor at the University of California Los Angeles at the age of 23, after wintering the previous year in Antarctica on a SCUBA research expedition with Scripps Institution of Oceanography, leading him to all seven continents before the age of thirty. During the intervening years, Paul received his masters and doctorate as a National Science Foundation graduate fellow at the Graduate School of Oceanography, University of Rhode Island. A decade later, he wrote the textbook on Science into Policy. As a Fulbright Distinguished Scholar at the University of Cambridge, he chaired the Antarctic Treaty Summit at the Smithsonian Institution in 2009, resulting in the first book on Science Diplomacy. Applying lessons of science diplomacy, the following year, as Head of the Arctic Ocean Geopolitics Programme at the University of Cambridge, he co-directed the first formal NATO-Russia dialogue regarding Environmental Security in the Arctic Ocean, which became the title of an edited book with over 60,000 downloads. He also co-convened the 1st and 2nd International Dialogue on Science and Technology Advice in Foreign Ministries in Austria (2016) and France (2017). He currently coordinates the Arctic Options and Pan-Arctic Options projects (involving national science agencies in the United States, Russian Federation, Norway, France, China and Canada from 2013-2020). Prof. Berkman joined the Fletcher School of Law and Diplomacy in 2015 as Professor of Practice in Science Diplomacy and is Founding Director of the Science Diplomacy Center at Tufts University, training science diplomacy among university networks as well as national diplomatic academies with common-interest building among nations, as reflected most recently with the Baseline of Russian Arctic Laws (2019). For his international, interdisciplinary and inclusive (holistic) contributions at global-local levels, Prof. Berkman has received awards in the United States, United Kingdom, Russian Federation, Norway, New Zealand and Japan. Paul is happily married with two daughters.

Methodology

The course will be delivered via the e-Learning platform Moodle (please see the course *User's Guide* for instructions on using this platform). This pedagogical tool will help the student meet the course's learning objectives through a self-paced study routine supported by multimedia, optional and required readings, discussion forums, assessment quizzes, and a wealth of other information. Adapted specifically to full-time professionals, students will learn by: absorbing (reading), doing (activities), interacting (socializing), and reflecting (relating to personal experience).

Materials will be posted online on a weekly basis. Your course is divided into six modules. All six modules contain the same structural elements:

- Lesson Material in form of a PDF document
- Lesson Material in form of interactive Articulate Storyline Files
- Discussion Board
- Assessment

Grading Policy and Course Completion

Students are eligible for a course certificate upon successful course completion. Successful completion requires:

- an 80% passing grade on EACH of the six module-based assessments (16 out of 20 questions correct); you may take each assessment up to 3 times (questions are randomized from a larger pool of questions and therefore will change upon assessment attempts); your best attempt counts;
- participation in the weekly Discussion Board forums; your posts will be evaluated according to both **quantity and quality** (e.g., content relevance and contribution to overall discussion).

Before moving to the next module, you should: **(a)** read all the core module texts, **(b)** take the module-based assessments, and **(c)** participate in the weekly Discussion Board forums. You are encouraged to consult the optional external links to enhance your knowledge of the given lesson's topic (e.g., links to websites and additional documents).

All assessments, once made available, will remain accessible until the end of the course and you can be taken anytime during the duration of the course, however assessments should be taken before moving to the next module.

UNITAR's e-Learning Committee will make the final decision regarding certificates in consultation with the moderator. UNITAR reserves the right to award certificates of completion only to those considered as "eligible" participants. We urge you to take a clear note of the above requirements. If you need any clarification, please do not hesitate to contact the Division for Multilateral Diplomacy Team.

Study Planning

The following study grid indicates which course activities are mandatory.

Activity	Mandatory
Interactive Course	Yes
External Links and Readings	No, recommended
Cybrary	No
Module Assessments	Yes
Discussion Forums	Yes
Course Evaluation	Yes

What is distinct about this learning experience is that it is an **online** learning experience. Online training, by its very nature, entails delivery of educational content over the internet. As you will proceed in this course, training materials will be made available to you through UNITAR's e-Learning portal. This course will also provide links to other web resources such as references and documents.

The UNITAR team is available to provide guidance and user information to help you participate and **contribute actively** to the discussion forums, which are an important requirement for completing this course. You will also have access to modules' moderators who will animate the discussion board as well as answer substantive and course related questions (either using the Discussion Board or through a traditional e-mail method).

The **advantages** of online training are many. You are able to:

- schedule and pace your learning according to your specific needs
- work from office or home as long as you have a computer with an internet connection
- connect with your fellow participants and instructors through the learning portal

The lack of face-to-face interaction will require more discipline and pro-active planning on your end in order to successfully meet the course's learning objectives. In this regard, it is thus different and distinct from a traditional face-to-face training course.

Although this online course is asynchronous – meaning that the interaction between you and the trainers or fellow participants will take place intermittently with a time delay – it will be important to establish a course study routine that best adapts to your work schedule, family commitments, Internet connection speed, etc. *Please note that the DMD e-Learning Team will send a reminder if your module-based assessments have not been completed.*

Learning Content

The complete set of course materials **will NOT be available all at once on the UNITAR portal. Materials will be posted on a weekly basis.** Learning materials are organised as follows:

1. Interactive Course

The interactive course is the core mandatory learning activity. The various module lessons contain links to external documents and websites, videos, questions and suggested responses, and basic text. The lessons are relevant to a wide demographic of participants, both those with basic knowledge on the topic as well as those with more advanced knowledge who wish to focus on the more specialized points of the course.

2. Cybrary

The Cybrary (Cyber Library) is the Resources section of this course. It contains both optional and mandatory materials to enhance your understanding of a given lesson's subject matter. It contains many additional resources, including:

- Printable PDF version of each module (with the Documents to Download cited in each module)
- Optional Readings
- Assessment Answers (posted at the end of the course)
- Transcripts of Videos
- Endnotes with links to many interesting Websites and Articles

Technical Support

For any technical issue or coordination matter, you may contact the Division for Multilateral Diplomacy e-Learning Team (DMD e-Learning Team) by sending a message through the UNITAR Virtual Learning Environment.

You may also contact us by email. Email support is available 24/7, and Emails will be answered within 24 hours.

MDP e-Learning Team

E-mail: julian.caletti@unitar.org

Phone: +41 22 917 8716

Office location: Geneva, Switzerland

Phone support hours: 8am to 5pm UTC/GMT