UNIVERSITY MODULE SERIES

Cybercrime

TEACHING GUIDE

UNODC | The Doha Declaration: PROMOTING A CULTURE OF LAWFULNESS

education for justice

UNITED NATIONS OFFICE ON DRUGS AND CRIME

EDUCATION FOR JUSTICE
UNIVERSITY MODULE SERIES

Cybercrime

TEACHING GUIDE

UNITED NATIONS
Vienna, 2019

This Teaching Guide is a resource for lecturers.

Developed under the Education for Justice (E4J) initiative of the United Nations Office on Drugs and Crime (UNODC), a component of the Global Programme for the Implementation of the Doha Declaration, this Guide forms part of the E4J University Module Series on Cybercrime. The full range of E4J materials includes university modules on integrity and ethics, crime prevention and criminal justice, anti-corruption, organized crime, firearms, trafficking in persons / smuggling of migrants, wildlife, forest and fisheries crime, counter-terrorism as well as cybercrime.

All the modules in the E4J University Module Series provide suggestions for in-class exercises, student assessments, slides and other teaching tools that lecturers can adapt to their contexts, and integrate into existing university courses and programmes. Each Module provides an outline for a three-hour class, but can be used for shorter or longer sessions.

All E4J university modules engage with existing academic research and debates, and may contain information, opinions and statements from a variety of sources, including press reports and independent experts. Links to external resources were tested at the time of publication. However, as third-party websites may change, please contact us if you come across a broken link or are redirected to inappropriate content. Please also inform us if you notice that a publication is linked to an unofficial version or website.

Terms and conditions of use of the Module can be found on the E4J website.

The designations employed and the presentation of material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries.

This publication has not been formally edited.

Content

Welcome message

Welcome to the Education for Justice (E4J) University Module Series on Cybercrime. The Cybercrime University Module Series development team has worked hard to find the most relevant, cross-cultural resources. Cybercrime is a growing, global problem. Whether you are a small business, a fortune 500 company, buying your first smartphone, or studying to be a cybersecurity expert, you need to be aware of cybercrime.

The Internet affords education and economic opportunities beyond anything the world has ever seen. This same tool, however, gives unprecedented opportunities to cause harm. By abusing technology, cybercriminals can ruin businesses and even lives. Many organizations around the world are fighting to stop cybercriminals and help to make systems more secure. However, one of the best methods of prevention is education.

The E4J University Module Series on Cybercrime brings together resources from around the world related to cybercrime, legislation, investigation and prevention. These Modules cover many aspects of this complex and fascinating field and include both theoretical concepts, as well as practical knowledge. The Modules provide themes and resources required for a rounded education on the various aspects of cybercrime, including cybercrime investigation and prevention.

The Modules are written with lecturers in mind by practicing educators. We have aimed to design a structure that provides the most support for building a new course, or a new series of courses, with as little effort as possible. We know building a new course on your own is difficult, especially in new areas of study like cybercrime. These Modules will give educators all the tools they need to build a great curriculum.

We envision an educator using these Modules to construct a course that best fits the needs of his or her students. We strive for each Module to be as self-contained as possible, while fitting

into an overarching theme. Educators are encouraged to use Modules from all available teaching guides to create a custom course that meets the educator's individual teaching goals. For example, Modules from the E4J University Module Series on Integrity and Ethics could be combined with some of the Cybercrime Modules in a practical cybersecurity and anti-cyberbullying course for students.

Technology and cybercrime evolve quickly. These Modules include core concepts needed to understand the problem of cybercrime. However, an educator should be aware of changes in the cybercrime landscape. This is especially true for local cybercrime legislation which is constantly being created and revised. For example, cyberbullying is such a new concept that many countries have not yet passed related legislation. More people than ever before have access to technologies such as smartphones, and if online harassment is not yet an issue being explored by lawmakers in your country, it likely will be in the future. Now is the time to teach the future generation how to respond to current and upcoming types of cybercrime in a healthy and safe way.

Further, states are examining their cyberwarfare options, and just like traditional warfare cyberwarfare will have negative consequences for civilians. Education on cybercrime issues can facilitate informed dialogue and peaceful resolutions of cyberconflict. The world, therefore, desperately needs a better understanding of the current state of cybercrime, cybersecurity, and cyberspace in general.

Cybercrime poses many challenges, but by working together we can make the Internet a safer, secure and more productive place. We would like to thank you, educators, for helping to teach the next generations about cybercrime and prevention.

Executive summary

The E4J University Module Series on Cybercrime provides lecturers with guidance and resources to build a comprehensive, cross-discipline course on cybercrime. The Modules within the series provide the themes and resources required for a rounded education on the various aspects of cybercrime and cybercrime investigation. The Modules cover cybercrime trends, theories, perspectives, laws, measures, and practices through a multidisciplinary lens.

The Teaching Guide and 14 Modules are the result of collaborative work from leading experts and academics from over 25 countries on six different continents. The Modules cover many aspects of this highly pertinent field and include both theoretical concepts as well as practical knowledge:

Module 1 serves as an introduction to cybercrime, including key concepts relating to computing, global connectivity, technology usage, and cybercrime trends, and the technical, legal, ethical, and operational challenges related to cybercrime, and cybercrime prevention.

Module 2 covers general categories of cybercrime, particularly offences against the confidentiality, integrity and availability of computer data and systems, computer-related offences, and content-related offences, and the types of cybercrimes included within these categories.

Module 3 describes the legal landscape relating to cybercrime, highlights the need for harmonized legislation, and outlines the relationship between cybercrime laws and human rights. Special attention is paid to the need for cybercrime laws to comply with human rights law, and any limitation of human rights to be in accordance with human rights standards and principles.

Module 4 provides an overview of digital forensics and electronic evidence, looking in particular at the digital forensics process, common digital forensics practices, standards for digital forensics and electronic evidence, and good practices in digital forensics.

Module 5 examines a multitude of stakeholders (i.e., agencies, organizations, businesses, and individuals) and their roles in cybercrime investigations, as well as the reporting of cybercrime, the challenges posed by cybercrime investigations, and the role of knowledge management in cybercrime investigations.

Module 6 discusses digital forensics and cybercrime investigations. This Module explores the legal and ethical obligations of cybercrime investigators and digital forensics professionals, good practices in the handling of digital evidence, its analysis, the reporting of digital forensics results, and the assessment of digital evidence.

Module 7 provides an in-depth exploration of international cooperation as it relates to cybercrime, particularly issues of sovereignty and jurisdiction, factors influencing international cooperation, formal and informal international cooperation mechanisms, extraterritorial evidence collection, and the national deficits in capacity to conduct cybercrime investigations.

Module 8 critically explores the cybersecurity strategies countries use to protect information and communication technology (ICT), the features and life cycles of these strategies, the frameworks used to assess these strategies and countries' cyber-related security and crime prevention efforts, and the nature and extent of countries' abilities to protect ICT.

Module 9 covers cybersecurity risks and risk-related concepts, cybersecurity research and vulnerability disclosure, situational crime prevention strategies and techniques, and usable cybersecurity measures that are designed to identify threats and vulnerabilities, and prevent, detect, respond to, and recover from materialized threats.

Module 10 critically examines the impact of data aggregation, as well as the impact of data collection, storage, analysis, use, and sharing, on privacy and security. Specifically, this Module covers privacy as a human right, the relationship between privacy and security, the ways in which cybercrime compromises privacy and data security, and data protection and breach notification laws, as well as the ways in which data is (and can be) protected to secure persons, property, and information.

Module 11 examines intellectual property and its cyber-enabled unauthorized access, distribution, and use. Specifically, this Module examines what intellectual property is, types of intellectual property, the causes, reasons, and perceived justifications for cyber-enabled copyright and trademark offences, and protective and preventive measures against such offences.

Module 12 focuses on interpersonal cybercrimes, including online child sexual abuse material, cyberstalking, cyberharassment, image-based sexual abuse, and cyberbullying, looking in particular at the gendered dimensions of these cybercrimes, the ways in which these cybercrimes are perpetrated, the laws targeting these cybercrimes, and global response and prevention efforts.

Module 13 examines the types of crimes that are considered as cyber organized crime and the types of organized criminal groups that engage in cybercrime. This Module further explores the measures used to counter cyber organized crime.

Module 14 examines topics, such as hacktivism, terrorism, espionage, disinformation campaigns, and warfare in cyberspace, as well as national and international perspectives and responses to these cyber activities. The purpose of this Module is to discuss these topics and identify current debates and conflicting views on these topics within and between countries.

The Modules, by design, contain elements that can be customized by lecturers from any country to suit their educational needs. While the E4J University Module Series on Cybercrime attempts to be as comprehensive as possible, one course can only lay the foundation of key concepts related to cybercrime. Each subtopic within the Module can be explored in much further detail and can even be expanded into its own course. Therefore, we have included optional resources for educators to advance their knowledge in related areas. The goal of these Modules is to advance global knowledge about cybercrime, including cybercrime investigation and prevention. While these Modules provide a strong foundation of cybercrime knowledge,

we encourage educators to add their own experiences and customize teaching material and examples to suit their local context in order to build the best possible educational content.

The purpose of this Teaching Guide is to explain the thought process behind the development of the Modules and what principles guided their development.

Introduction

Education for Justice (E4J) was developed as part of UNODC's Global Programme to support key objectives of the Doha Declaration on Integrating Crime Prevention and Criminal Justice into the Wider United Nations Agenda to Address Social and Economic Challenges and to Promote the Rule of Law at the National and International Levels, and Public Participation (the Doha Declaration), which was adopted by the Thirteenth United Nations Congress on Crime Prevention and Criminal Justice in 2015 and endorsed by the United Nations General Assembly in its Resolution 70/174 (A/RES/70/174). The Declaration recognizes the fundamental importance of universal education for children and youth as key to the prevention of crime, terrorism, and corruption, as well as to promote sustainable development.

The E4J initiative is aimed at building a culture of lawfulness among children and youth through the provision of age-appropriate educational materials on topics related to criminal justice, crime prevention, and the rule of law, and the integration of those materials into the curricula of all education levels. At the university level, E4J provides support to academics in their teaching and research activities related to UNODC mandate areas, including crime prevention and criminal justice, anti-corruption, organized crime, trafficking in persons and smuggling of migrants, firearms, cybercrime, wildlife, forest and fisheries crime, counter-terrorism as well as integrity and ethics. This Module Series covers one of these mandate areas; namely cybercrime.

Few personal and professional activities have remained unaffected by information and communication technology (ICT). For this reason, the education of users of ICT is essential. Education of users is also critical considering the current worldwide deficit in capacity to deal with cybercrime and cybersecurity-related issues (UNODC, 2013; Frost & Sullivan Executive Briefing, 2017). Assessment tools and frameworks that have been developed to assess the cybersecurity capabilities of countries, organizations, and businesses clearly demonstrate this (see Cybercrime Module 8 for more information).

Cybercrime requires a multifaceted response combining education, laws, social awareness, training of law enforcement agencies, and the cooperation of Internet intermediaries, among

others. Accordingly, the deficits in national capacity need to be filled by educating current and next generations of professionals and opening up cybercrime and cybersecurity education to professionals outside of the fields of criminal justice, law, and computer science. In fact, the current deficit exists because of a lack of multidisciplinary focus on cybercrime and cybersecurity. To fill this void, the Cybercrime Module Series utilizes a multidisciplinary approach to analyse core cybercrime issues, cybersecurity strategies and measures, digital evidence, digital forensics, cybercrime laws, and investigative practices. Particularly, the Modules cover good cybercrime prevention and cybersecurity practices identified by countries around the world in the 2013 UNODC Draft Comprehensive Study on Cybercrime. These best practices include the development of a strong cybercrime and cybersecurity knowledge base; education and awareness campaigns; criminal justice capacity, in general, and law enforcement capacity, in particular; national, regional, and international cybercrime legal frameworks and their harmonization; and international cooperation between national, regional, and international agencies and organizations, as well as the private sector, on cybercrime matters.

The interconnectedness and interdependency of societies has provided immeasurable opportunities for economic growth, employment, and interpersonal communications and connections. And yet, this interconnectedness and interdependency has created numerous vulnerabilities that can (and have been) exploited by a variety of actors no longer restricted by time and space in committing illicit activity. These cybercriminals can commit cybercrime irrespective of geographic location at any time and any place anywhere in the world with an Internet connection. For these reasons, cybercrime prevention and cybersecurity are of paramount importance.

In addition to exploring cybercrime prevention and cybersecurity, the Modules also cover core cybercrime-related topics, such as privacy and data protection. Not only does privacy and data protection safeguard individuals from cybercrime by shielding them and their data from cybercriminals, but they also facilitate and enable individuals' exercise of their human rights online. These Modules also introduce critical cybercrime and cybersecurity issues, causes of and factors influencing cybercrime, and the motives, tactics, targets, and methods of operation of cybercriminals, as well as what makes individuals, businesses, and governments targets of cybercrime, and what can be done to prevent cybercrimes and protect these targets from cybercrime.

The E4J University Module Series on Cybercrime includes the following Modules:

- Module 1: Introduction to cybercrime
- Module 2: General types of cybercrime
- Module 3: Legal frameworks and human rights
- Module 4: Introduction to digital forensics

- Module 5: Cybercrime investigation
- Module 6: Practical aspects of cybercrime investigations and digital forensics
- Module 7: International cooperation against cybercrime
- Module 8: Cybersecurity and cybercrime prevention: strategies, policies, and programs
- Module 9: Cybersecurity and cybercrime prevention: practical applications and measures
- Module 10: Privacy and data protection
- Module 11: Cyber-enabled intellectual property crime
- Module 12: Interpersonal cybercrime
- Module 13: Cyber organized crime
- Module 14: Hacktivism, terrorism, espionage, disinformation campaigns, and warfare in cyberspace

Please note that the Module sequence is designed to provide a foundational knowledge and can be changed in a flexible and modular manner depending on the expected level of the class. The Modules blend theories, research, and practice and were developed in consultation with a group of educational experts. All Modules combine practical and theoretical approaches to the specific cybercrime topics and follow the same basic structure:

Introduction. Each Module includes an introduction, which is used to establish the interest, need and purpose of the content, and provides an overview of the topic or topics covered.

Learning Objectives. Each Module includes the expected module objectives in the form of learning outcomes, which cover the observable expected outcomes of learning (learning objectives are explored in greater detail in the next section of this Teaching Guide, "5.3. Learning Outcomes and Assessment Tools").

Key Issues. Each Module highlights fundamental topics regarding the Module. Boxes with interesting cases and research topics and questions that highlight critical cybercrime issues (e.g., thematic and "Did you know?" boxes), as well as laws, interesting examples, and notes on the topics are included in the Modules. This section of the Module also includes reference lists for academic and professional literature and research cited within the Module, as well as a list of cases and laws referenced within the Modules.

Exercises. The exercises in each Module are designed to stimulate students' problem solving and critical thinking skills. They are also used to assess student learning and enable students to apply what they learned in the class (these exercises are explored in greater detail in the next section of this Teaching Guide, "5.3. Learning Outcomes and Assessment Tools"). There is scope for lecturers to adapt and customize these exercises to match their local requirements and context.

Core and Advanced Reading. Each Module has core and advanced reading. The core reading contains prescribed core literature on the subject and the material covered in the Module and are to be used for the class or course development. The advanced reading includes further information on the topics covered in the Module, which can be used to explore topics in more depth, supplement core reading, develop other classes or entire courses on the topics covered, and/or to tailor the content to the academic backgrounds of the students in the class and/or the academic discipline associated with the course. Lecturers can mix and match readings based on their needs, abilities, and preferences, as well as their access to the readings.

> *Did you know?*
>
> UNODC's Education for Justice (E4J) initiative has a Library of Resources, which includes open access educational material. For more information, visit: http://www.unodc.org/e4j-library.

These core and advanced reading include open and closed source publications. *Open source publications* are available for free and without the need of a special license or purchase of the work. These core and advanced readings include the links where the publication can be accessed. *Closed source publications* include academic journal articles and books that are only available through subscriptions to academic journal databases (e.g., Taylor and Francis, Sage, Jstor, Springer, and Wiley, to name a few) or for purchase. There are, however, exceptions to this. For academic journal articles, the authors of the articles can be contacted, and a request can be made for the work (authors' contact details are included in the articles). These articles may also be posted on research sharing sites like ResearchGate and Academic.edu. If the full text of the articles are not posted on these sites, authors on these sites may be contacted to requests this information as long as the requests respect national intellectual property laws. For books, the authors of these books can be contacted to request a copy of their book for donation to a university or college library.

> *Note*
>
> Most of the core and advanced readings are in English. UNODC can be contacted for assistance on the translation of these publications into other languages.

Possible Class Structure. Every Module includes a possible class structure that incorporates multiple modalities of learning and the suggested sequence of topics and activities. The lecture is meant to reinforce what students learned in the readings and the exercises and other student assessment activities are designed to apply what they learned in the readings. The breakdown in the Modules is designed based on a three-hour class. The lecturers can adapt the structure based on their needs and the class times. Each Module was designed to

incorporate approximately twelve notional hours of learning (roughly six hours of preparation time, three hours of class attendance, and three hours of assessment/assignments). However, it is possible for individual lecturers to extend the content into more than one class or an entire course.

Student Assessment. In addition to the exercises, each Module includes review questions to assess students' learning, and other forms of assessment, such as homework assignments, case studies, group assignments, and "Knowledge Check" prompts, which ask students to answer a question based on information provided to assess students' recall and comprehension of information (students assessment is explored in greater detail in the next section of this Teaching Guide, "5.3. Learning Outcomes and Assessment Tools").

Additional Teaching Tools. Each Module contains additional teaching tools that can be used within the course, such as important websites, which include background information to the material covered in the Module, similar material to that covered in the Module, and/or further information than that covered in the Module, and videos, which are meant to highlight certain parts of the Module and can be used at the lecturer's discretion to highlight key issues identified in the Module and/or to illustrate topics covered in the Module (these teaching tools are explored in greater detail in the next section of this Teaching Guide, "5. Teaching and Learning Methods").

The Modules are not all-inclusive in content. The Modules are simply designed to highlight key issues relating to the topics covered in the Modules and to assist lecturers in teaching those topics by providing a basic framework for the lecture and recommending exercises, assignments, and core and advanced readings for faculty, students, and others interested in learning about cybercrime and related topics. The Modules have not been designed specifically for cybercrime majors, but for every lecturer who is interested in integrating cybercrime-related materials into courses of other academic disciplines and/or adding and/or creating new cybercrime-related courses to academic programmes. The Modules can be used by lecturers from multiple disciplines at the undergraduate and graduate level.

Teaching and learning methods

The E4J University Modules on Cybercrime provide materials and pedagogical tools to help lecturers teach classes on cybercrime and cybercrime-related topics. The Modules were designed with learning styles, multiple modalities of learning, learning outcomes, and student assessment tools in mind.

Learning styles

Individuals learn and retain information differently. Because of this, courses should accommodate various forms of learning. The Cybercrime Modules are designed to accommodate various learning styles, which refers to the way information is understood, recalled, expressed, applied, synthesized, and assessed. There are several learning styles, among them are visual, auditory, read/write, and kinaesthetic (a.k.a., VARK modalities; Fleming and Mills, 1992):

- ***V**isual* learners learn with their eyes; that is, they learn based on what they see, be it PowerPoint Slides, figures, charts, schematics, images, or videos (to name a few).

- ***A**uditory* learners learn with their ears. These learners consume and process information that is heard such as lectures (i.e., is a form of discourse where information is presented, explained, and analysed) or discussions.

- ***R**ead/write* learners, as the name implies, learn by reading material and taking notes on the material.

- ***K**inaesthetic* learners learn by engaging in a task (i.e., doing something); that is, they learn by applying what they learned in case studies and practical exercises.

The belief is that students have preferred learning styles and that instruction should be tailored to these learning styles. However, this theory is not well-supported in the literature (Brown, McDaniel and Roediger, 2014).

Want to learn more about research in teaching and learning in higher education?

Read:

Ambrose, Susan, Michael W. Bridges, Michele DiPietro, Marsha C. Lovett, and Marie K. Norman. (2010). *How Learning Works: Seven Research-Based Principles for Smart Teaching*. Jossey-Bass.

Bain, Ken. (2004). *What the Best College Teachers Do*. Harvard University Press.

Brown, Peter, Mark McDaniel, and Henry L. Roediger. (2014). *Make It Stick: The Science of Successful Learning*. Harvard University Press.

Lang, James M. (2016). *Small Teaching: Everyday Lessons from the Science of Learning*. Jossey-Bass.

Segal, Mark (2013). *How To Train: A Practical Guide for Training and Working with Others*

Angele Attard, Emma Di Iorio, Koen Geven, Robert Santa (2010). *Student-Centred Learning - Toolkit for students, staff and higher education institutions*

While it is true that some students prefer to read or listen to lectures while others like to engage in discussions or write, no evidence supports the idea that students learn more effectively when they are working in their own preferred learning style. Indeed, some researchers have discovered that students are often mistaken when they predict the type of activity that produces the greatest learning for them. Indeed, learning is most effective when it requires some effort on the part of the student, which means that students might learn more effectively when they are required to engage in activities that they find challenging.

All of this leads to an important conclusion about the kinds of engagement activities that should be designed for students: *they should be varied*. If the lecturer does nothing but lecture to students, those students who do not respond very well to lectures - because they have difficulty paying attention for long periods of time, for example - are at a disadvantage. Likewise, if the lecturer does nothing but have students engage in debates, those students who like to have the opportunity to read or listen quietly to an expert are at a disadvantage. As lecturers are putting together plans to teach any of the Modules, they should consider how to offer varied methods for students to engage actively with the learning material. All the Cybercrime Modules contain within them recommendations for active engagement in different forms.

Metacognition

"Metacognition refers to individuals' ability to understand their knowledge levels and learning abilities" (E4J Integrity and Ethics Teaching Guide).

Want to learn more?

See:

- E4J Integrity and Ethics Teaching Guide.
- How to Get the Most Out of Studying: Part 1 of 5, "Beliefs That Make You Fail... Or Succeed," https://www.youtube.com/watch?v=RH95h36NChI.
- How to Get the Most Out of Studying: Part 2 of 5, "What Students Should Know About How People Learn," https://www.youtube.com/watch?v=9O7y7XEC66M.
- How to Get the Most Out of Studying: Part 3 of 5, "Cognitive Principles for Optimizing Learning," https://www.youtube.com/watch?v=1xeHh5DnCIw.
- How to Get the Most Out of Studying: Part 4 of 5, "Putting Principles for Learning into Practice," https://www.youtube.com/watch?v=E9GrOxhYZdQ.
- How to Get the Most Out of Studying: Part 5 of 5, "I Blew the Exam, Now What?" https://www.youtube.com/watch?v=-QVRiMkdRsU.

Multiple modalities of learning

The Modules accommodate multiple learning styles by including lectures, discussions, exercises, case studies, hypothetical scenarios, review questions, homework assignments, and additional technical tools, such as videos and websites. Lectures, as well as the viewing of videos, promote *passive student learning*. To promote *active student learning*, lectures should incorporate discussions, exercises, case studies, hypothetical scenarios, review questions, among other assignments (see, for example, Berkeley Center for Teaching & Learning, and Yale Poorvu Center for Teaching and Learning). Because some students prefer to work alone (*solitary* learners) and others in groups (*social* learners), both individual and group assignments are included in the Cybercrime Module Series. Accordingly, multiple modalities of learning are incorporated in the Modules to reflect this variation in learning styles and promote passive and active learning.

Note

Lecturers can adapt the exercises and assignments included in the Cybercrime Module Series to include other active learning techniques.

For more information about these techniques, see:
Berkeley Center for Teaching & Learning, Active Learning Strategies, https://teaching.berkeley.edu/active-learning-strategies.
Yale Poorvu Center for Teaching and Learning, Active Learning, https://poorvucenter.yale.edu/ActiveLearning.

The Modules are based on participatory learning (i.e., learning by problem solving using own experience and skills) and experiential learning (i.e., learning through experience) models, which promotes mutual and active learning, student empowerment, and critical reflections on ideas and practice. The Modules were designed this way to stimulate forms of thinking beyond basic recall and memorization of content (i.e., critical thinking skills). Benjamin Bloom, an educational psychologist, developed a taxonomy of cognitive development in 1953 (known as Bloom's taxonomy), which includes a range of cognitive skills and is widely used in academia. Bloom's (1953) taxonomy identifies six cognitive levels or domains: *knowledge* (i.e., ability to remember information); *comprehension* (i.e., ability to understand information); *application* (i.e., ability to use what they learned); *analysis* (i.e., ability to analyse information); *synthesis* (i.e., ability to combine what was previously known with other information learned to create new knowledge), and *evaluation* (i.e., ability to judge information) (see Figure 2). These cognitive skills cover essential skills, such as *problem solving* (i.e., the ability to recognize a problem, identify strategies to solve a problem by proposing solutions, evaluating these solutions considering available contextual information, and assessing the outcomes of proposed solutions), and *creative thinking*, whereby individuals combine existing knowledge, skills and abilities in new and/or unique ways to solve problems or resolve issues.

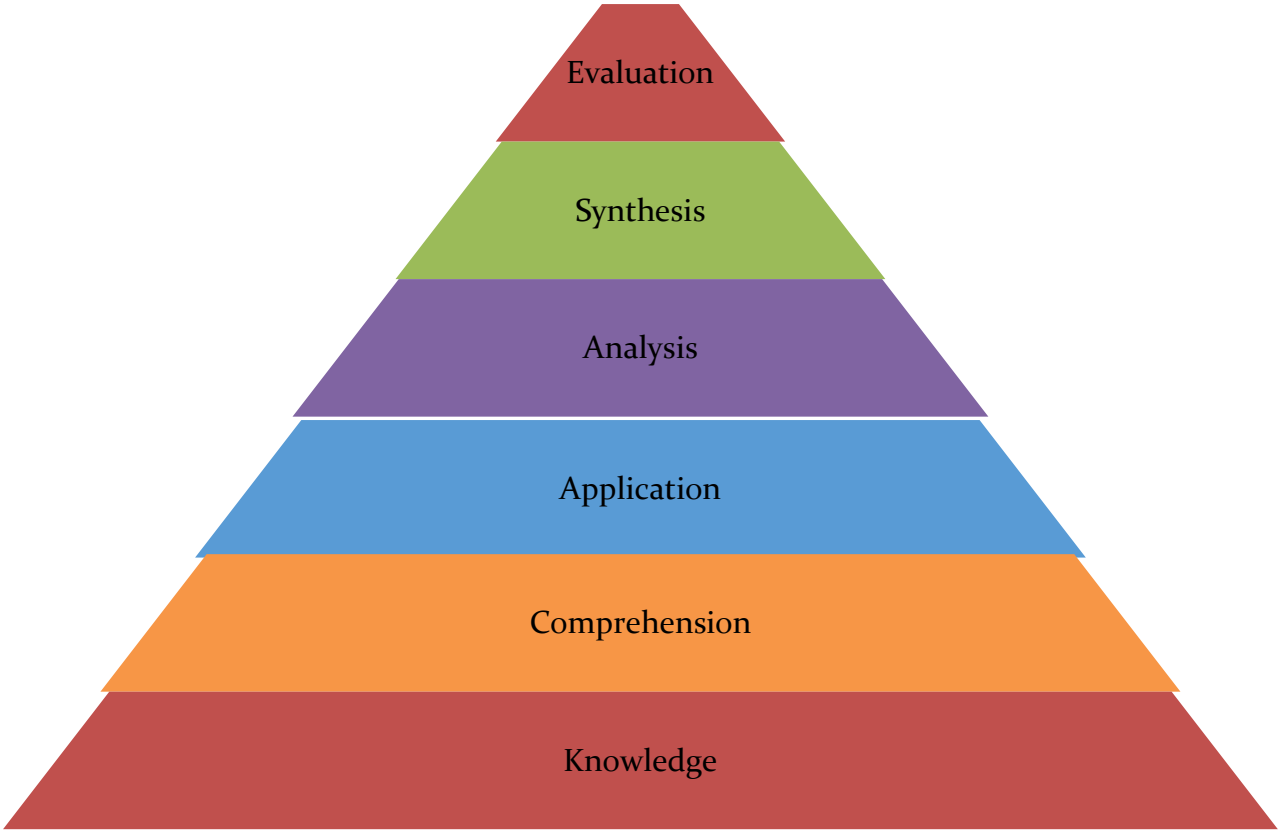

Figure 2 Bloom's taxonomy (1953)

Bloom's taxonomy was revised in by Anderson and Krathwohl in 2001 (Figure 3), covering a range of cognitive skills from the lowest-level of thinking to the highest: *remembering*, *understanding*, *applying*, *analysing*, *evaluating*, and *creating*. Bloom's original and revised taxonomy explain student learning.

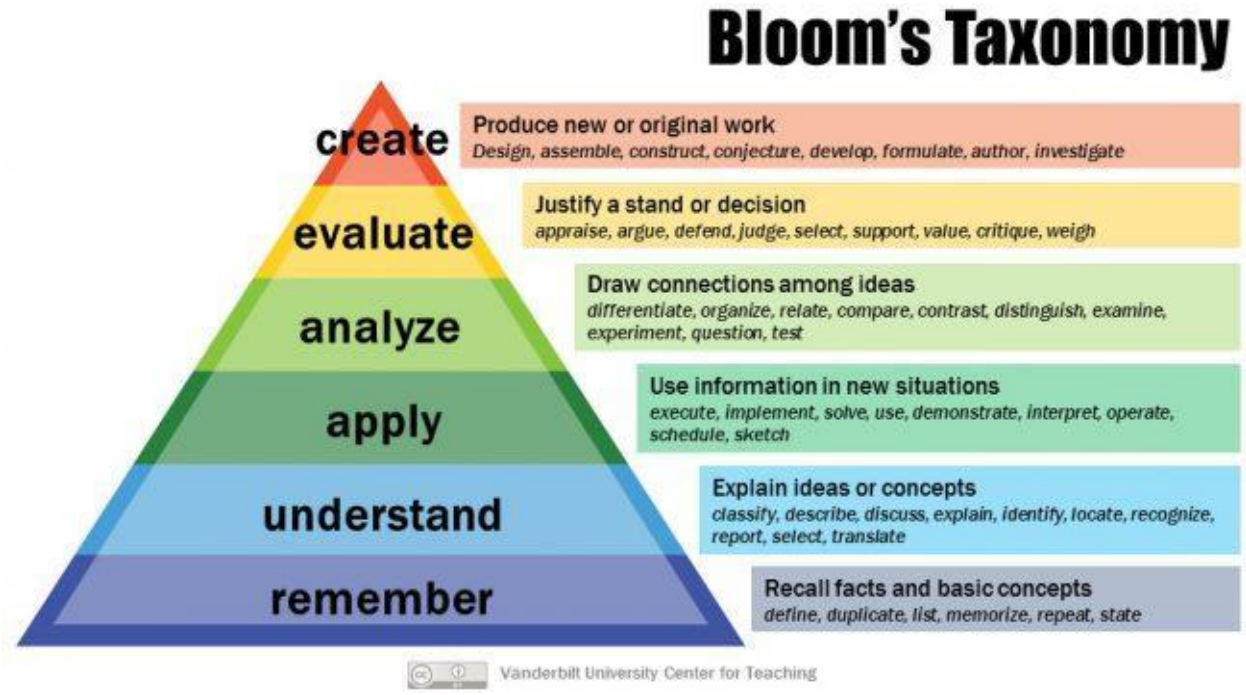

Figure 3 Bloom's revised taxonomy (2001)

Learning outcomes and assessment tools

The learning outcomes identify students' knowledge, attitudes, skills, and abilities by prescribing the type of behaviour students should be able to perform by the end of the course. Learning outcomes based on the revised Bloom's taxonomy (Anderson and Krathwohl, 2001) identify the following expectations for students' academic performance: learners are required to demonstrate that they know something (*remember*), comprehend something (*understand*), can apply what they learned (*apply*), can analyse information (*analyse*), can assess information (*evaluation*), and can develop something new (*create*).

The learning outcomes contain the observable outcome that is expected of the student and which can be demonstrated by the assessment tools used in the course. *Learning objectives* delineate what students *should* learn in the course (i.e., what they *should* be *able to do* at the end of the course). The *assessment tools* determine if and to what extent the learning objectives were met. It is thus imperative that learning objectives and assessment tools are aligned. Put simply, the content of the assessment tools should match the objectives being assessed.

There are several assessment tools that can be used to evaluate student learning. These assessment tools can be designed to objectively assess student behaviour or subjectively assess behaviour (Schwartz, n.d.; Center for Advanced Research on Language Acquisition, n.d.). *Objective assessments* require students to choose a response from options provided (Schwartz, n.d.). These types of assessments include *multiple choice questions*, where students choose one of the available answers provided to a question prompt or statement, or *true or false questions*, whereby students determine the veracity of a statement (Center for Advanced Research on Language Acquisition, n.d.). Objective assessments are primarily aimed at examining students' ability to recognize correct content and if designed correctly, to understand content (Schwartz, n.d.). It is important to note that objective assessments can also access other cognitive skills if designed correctly (Schwartz, n.d.).

Subjective assessments, by contrast, can assess multiple learning outcomes beyond those commonly evaluated by objective assessments, particularly those based on cognitive skills such as analysis, evaluation, and creation (Schwartz, n.d.). These types of assessments include case studies, exercises, homework, and review questions (Schwartz, n.d.). In the Modules, review questions, for example, are designed to assess students' abilities to recall, understand, apply, analyse, evaluate, and/or create information. The review questions are a form of subjective assessment. Some review questions have short answers designed to assess their abilities to

recall information, and long answers which are designed to assess ability to recall, analyse, evaluate, organize and synthesize material in response to questions. Students are also provided with exercises, case studies, hypothetical scenarios to "apply" the theories and concepts they learn to cybercrime cases and scenarios, and to assess current solutions and develop responses to cybercrime.

Need help in creating learning outcomes and student assessment tools?

Numerous academic institutions provide guidance on the development of learning outcomes and students assessment tools based on Bloom's taxonomy (original and revised). Guidance on the language to be used in drafting the learning outcomes (and what to avoid) is provided as well. Some examples of these websites are:

- Iowa State University, Center for Excellent in Teaching and Learning, Revised Bloom's Taxonomy. http://www.celt.iastate.edu/teaching/effective-teaching-practices/revised-blooms-taxonomy/.
- University of Toronto, Center for Teaching Support & Innovation, Writing Learning Outcomes Using Bloom's Revised Taxonomy. https://teaching.utoronto.ca/wp-content/uploads/2015/08/Learning-Outcomes-Using-Blooms-Taxonomy.pdf.
- Utica College, Bloom's Taxonomy of Measurable Verbs. https://www.utica.edu/academic/Assessment/new/Blooms%20Taxonomy%20-%20Best.pdf.

Ultimately, teaching should accommodate multiple learning styles and include multiple modalities of learning to inspire students to actively participate in courses by responding to discussion questions (which are aimed at verifying their comprehension of the course material), participating in group assignments, and applying and explaining their knowledge through exercises, review questions, and homework assignments.

Module adaptation and design guidelines

The E4J University Modules on Cybercrime have deliberately been designed to be adapted. Each Module provides an outline for a three-hour class but can be used for shorter or longer sessions. The following paragraphs provide examples of the kind of adaptation that can take place. It is not an exhaustive list and can be expanded where required.

To be able to support lecturers even further, UNODC would appreciate receiving any adapted versions of the E4J Modules (messages should be sent to e4j.cyberprevent@un.org). E4J will then share these with its network lecturers as examples of how the Modules can be adapted to different regions, contexts, and disciplines.

Localizing the content

The lecturer can take the following steps to localize the content:

- Determine if there is any content that might be deemed offensive in a local cultural context and remove or adapt that part
- Provide a customized introduction that refers to relevant legal frameworks and case studies, perhaps recent examples that appeared in local media
- If required, replace or complement the existing readings, case studies, and exercises with examples that reflect the local context
- If required, translate the content into local language
- Adapt content to better relate to a certain discipline, sector or industry

Integrating within an existing course

All E4J Modules have been designed in a way that they could either be offered as a stand-alone module or integrated within an existing course. As mentioned before, the modular structure allows lecturers to select only those that are relevant within a specific context. Lecturers have many options to use an E4J Module. As a stand-alone module, it could be offered as either a voluntary or mandatory addition to a course; for example, as a workshop offered outside the normal scheduled sessions. It could also be offered as part of summer/winter or interim sessions or as public sessions with broader participation than simply the registered students.

Integration of a Module within an existing course requires advanced planning, because a specific session would have to be scheduled in a course outline, which, depending on the academic institution, may have to go through internal approval processes. Nevertheless, lecturers often have substantial flexibility to introduce new, but related, content in a course outline. For example, in a transnational crime, crime, or criminology course there is likely to be an existing focus on cybercrime. In such a case, the lecturer can either replace the existing content with the E4J Module or adapt/merge the existing content with the E4J content. If there is no existing cybercrime content, the lecturer will have to rearrange the current content to create space in the course outline for the E4J material. It remains the responsibility of the lecturer to familiarize herself or himself with the academic requirements of the specific institutions. The process described above might not always be possible.

Changing the timeframe

The three-hour time slot is offered as a guideline. Depending on the lecturing style and the class size a typical E4J Module, with all exercises, student assessment, and/or additional teaching tools, could be offered in a three-hour timeframe. These timeframe requirements for classes vary between institutions and programmes. Undergraduate contact sessions are usually shorter and spread across more than one day a week. For this reason, the content of one E4J Module might have to be spread over two or more sessions. By contrast, graduate contact sessions could last two or three hours, which might be enough to cover the content of an entire Module. However, some lecturers may still wish to spread the Module over two sessions, as the break in between the two sessions could allow students to process and internalize the materials better. In some cases, lecturers might wish to introduce additional content to offer a half-day or even a full-day workshop. There are no rigid guidelines in this regard and lecturers should make adjustments that fit their circumstances.

Developing a stand-alone course

Each Module of the Cybercrime Series has a section called “Possible Class Structure” that is described as follows: “The following is a recommended structure for the class. Students should complete the core readings before coming to class. The lecture is meant to reinforce what they learned in the readings and the exercises are designed to apply what they learned in the readings. The following breakdown is designed based on a three-hour class. Lecturers can adapt the structure based on their needs and the class times.” The “Possible Class Structure” sections within the Cybercrime Module Series are very flexible and provide some high-level

suggestions on the content and structure of a stand-alone course. They can also be used to provide ideas for adding content to longer sessions or workshops.

Lecturers might wish to deliver combinations of the available Modules and/or may combine content from different Cybercrime Modules to create a course. Combinations will be determined by institutional or faculty requirements and informed by thematic priorities. Lecturers could also consider combinations involving E4J Modules in other areas. It is recalled in this context that E4J also offers University Module Series on the core mandates of UNODC, including integrity and ethics, anti-corruption, crime prevention and criminal justice, organized crime, trafficking in persons/smuggling of migrants, firearms, wildlife, forest and fisheries crime, and counter-terrorism. Given the availability of E4J University Module Series on a variety of subject areas and topics, and in the context of the myriad of possibilities provided by different timeframes, the entire E4J Cybercrime Module Series is adaptable to many different environments.

Overview of the Cybercrime Modules

All 14 of the Cybercrime Modules are freely available on the E4J website. UNODC offers them as open educational resources (OER) to assist lecturers in preparing and delivering university classes on cybercrime. Users may visit the E4J website and download and copy the information, documents and materials for non-commercial use. For tracking purposes, UNODC would appreciate being informed about the way in which the material was used and how many students were involved (messages should be sent to e4j.cyberprevent@un.org). Users can also contact E4J or register on the E4J website to receive news updates.

Summaries of all Modules, including learning outcomes and the mapping of assessment tools to learning outcomes are included below (click on the hyperlink included in the title to access the full Module).

Module 1: Introduction to Cybercrime

Information and communication technology (ICT) has transformed the way in which individuals conduct business, purchase goods and services, send and receive money, communicate, share information, interact with people, and form and cultivate relationships with others. This transformation, as well as the world's ever-increasing use of and dependency on ICT, creates vulnerabilities to criminals and other malicious actors targeting ICT and/or using ICT to commit crime. This Module introduces key concepts relating to cybercrime, what cybercrime is,

Internet, technology and cybercrime trends, and the technical, legal, ethical, and operational challenges related to cybercrime and cybercrime prevention.

Learning outcomes

L1 Define and describe basic concepts relating to computing
L2 Describe and assess global connectivity and technology usage trends
L3 Define cybercrime and discuss why cybercrime is scientifically studied
L4 Discuss and analyse cybercrime trends
L5 Identify, examine, and analyse the technical, legal, ethical, and operational challenges relating to the investigation and prevention of cybercrime

Assessment of student learning

Learning Outcomes	Bloom's Taxonomy (Original/Revised)	Assessment Tools
L1	Knowledge/Remembering Comprehension/Understanding	Exercise #1; Assignment; Review Questions; Class Discussions
L2	Knowledge/Remembering Comprehension/Understanding Evaluating	Exercise #2; Exercise #3; Review Questions; Class Discussions
L3	Knowledge/Remembering Comprehension/Understanding	Review Questions; Class Discussions
L4	Knowledge/Remembering Comprehension/Understanding Analysing	Review Questions; Class Discussions
L5	Comprehension/Understanding Applying Analysing	Exercise #4; Review Questions; Class Discussions; Case Study

Module 2: General Types of Cybercrime

Cybercrime includes "new" crimes – those made possible because of the existence of information and communication technology (ICT) – such as offences against the confidentiality, integrity and availability of computer data and systems, and traditional crimes facilitated in some way by ICT, which include computer-related offences and content-related offences. This Module covers different types of cybercrime, particularly cybercrimes that are considered

offences against the confidentiality, integrity and availability of computer data and systems, computer-related offences, and content-related offences.

Learning outcomes

L1 Define general types of cybercrime
L2 Identify and discuss the categories of cybercrime and the cybercrimes included within these categories
L3 Differentiate between different forms of cybercrime
L4 Describe and explain the ways in which certain cybercrimes are perpetrated

Assessment of student learning

Learning Outcomes	Bloom's Taxonomy (Original/Revised)	Assessment Tools
L1	Knowledge/Remembering	Review Questions; Class Discussions
L2	Knowledge/Remembering Comprehension/Understanding Applying Evaluating	Exercise #1; Exercise #2; Homework #1; Homework #2; Review Questions; Class Discussions
L3	Analysing	Exercise #1; Review Questions; Class Discussions
L4	Comprehension/Understanding Analysing	Review Questions; Class Discussions

Module 3: Legal Frameworks and Human Rights

National, regional, and international laws can govern behaviour in cyberspace and regulate criminal justice matters relating to cybercrimes. These laws not only set rules and expectations for behaviour, but also the procedures to be followed if the rules are broken, and behaviour expectations are not met. However, core cybercrime offences in national laws are not harmonized between countries, complicating international cooperation in criminal justice matters (discussed in detail in Cybercrime Module 7 on International Cooperation against Cybercrime and in the E4J University Module Series on Organize Crime, particularly Module 11 on International Cooperation to Combat Transnational Organized Crime).

The focus of this Module is to describe the legal landscape relating to cybercrime, highlight the need for harmonized legislation, and outline the relationship between cybercrime laws and

human rights. As this Module shows, cybercrime laws need to be in compliance with human rights law, and any limitation of a human right needs to be in accordance with human rights standards and principles.

Learning outcomes

L1 Identify, discuss, and examine the need for and role of cybercrime laws
L2 Describe and differentiate between substantive, procedural, and preventive cybercrime laws
L3 Identify and critically assess national, regional, and international cybercrime laws
L4 Critically evaluate the protection of human rights online

Assessment of student learning

Learning Outcomes	Bloom's Taxonomy (Original/Revised)	Assessment Tools
L1	Knowledge/Remembering Comprehension/Understanding Analysing	Exercise #2; Web Exercise; Review Questions; Class Discussions
L2	Knowledge/Remembering Analysing	Group Exercise; Review Questions; Class Discussions
L3	Knowledge/Remembering Comprehension/Understanding Evaluating	Review Questions; Class Discussions
L4	Evaluating	Exercise #1; Exercise #3; Knowledge Check; Review Questions; Class Discussions

Module 4: Introduction to Digital Forensics

Digital forensics refers to the process of retrieval, preservation, analysis, and presentation of *electronic evidence* for use in investigations and prosecutions of various forms of crime, including cybercrime. This Module provides an overview of digital forensics and electronic evidence, looking in particular at the digital forensics process, common digital forensics practices, standards for digital forensics and electronic evidence, and best practices in digital forensics.

Learning outcomes

L1 Discuss data and identify data sources
L2 Describe and discuss digital evidence
L3 Compare and contrast the differences between digital evidence and traditional evidence
L4 Discuss the ways in which digital evidence is authenticated
L5 Describe and critique digital forensics process models
L6 Critically evaluate standards and best practices for digital evidence and digital forensics

Assessment of student learning

Learning Outcomes	Bloom's Taxonomy (Original/Revised)	Assessment Tools
L1	Knowledge/Remembering Comprehension/Understanding	Exercise #1; Review Questions; Class Discussions
L2	Knowledge/Remembering Comprehension/Understanding	Review Questions; Class Discussions
L3	Analysing	Review Questions; Class Discussions
L4	Comprehension/Understanding Evaluating	Group Exercise; Review Questions; Class Discussions
L5	Knowledge/Remembering Comprehension/Understanding Evaluating	Review Questions; Class Discussions
L6	Evaluating	Exercise #2; Assignment; Review Questions; Class Discussions

Module 5: Cybercrime Investigation

There are a multitude of stakeholders (i.e., agencies, organizations, businesses, and individuals) that are involved in the investigation of cybercrime. The nature and extent of their involvement depends on the type of cybercrime committed. Stakeholder involvement is also determined by the geographic location of stakeholders and countries' cybercrime laws. Building on Module 4 on Introduction to Digital Forensics, Module 5 critically examines the processes involved in reporting cybercrime and the stakeholders responsible for investigation cybercrime. Special

attention is paid to the obstacles encountered during cybercrime investigations (for information on international cooperation in cybercrime investigations, see Module 7 on International Cooperation against Cybercrime and the E4J University Module Series on Organized Crime, particularly Module 11 on International Cooperation to Combat Transnational Organized Crime) and the role of knowledge management in cybercrime investigations. Module 6 on Practical Aspects of Cybercrime Investigations and Digital Forensics covers the way cybercrime investigations and digital forensics are conducted.

Learning outcomes

L1 Discuss and assess cybercrime reporting practices
L2 Identify and discuss the stakeholders involved in cybercrime investigations
L3 Explain and critically evaluate the resources leveraged during a cybercrime investigation and the obstacles encountered by investigators
L4 Describe and appraise the role of knowledge management in cybercrime investigations

Assessment of student learning

Learning Outcomes	Bloom's Taxonomy (Original/Revised)	Assessment Tools
L1	Comprehension/Understanding Evaluating	Review Questions; Class Discussions
L2	Knowledge/Remembering Comprehension/Understanding	Homework #1; Exercise #1; Exercise #3; Review Questions; Class Discussions
L3	Applying Analysing Evaluating	Exercise #2; Homework #2; Review Questions; Class Discussions
L4	Comprehension/Understanding Analysing Evaluating	Exercise #3; Review Questions; Class Discussions

Module 6: Practical Aspects of Cybercrime Investigations and Digital Forensics Introduction

When investigating crimes, law enforcement agencies are more likely than not to encounter information and communication technology (ICT) during an investigation. ICT can be the target of the cybercrime, used to commit a cybercrime, or contain evidence of a crime. ICTs and the

data within them are examined to identify evidence of criminal activity. The investigation seeks to scientifically establish the facts of a case using digital evidence. The investigator's role is to identify this evidence and reconstruct the sequence of events of the crime (or cybercrime) or that leads to the crime (or cybercrime). This Module examines the way digital evidence is identified, particularly digital forensics (discussed in Cybercrime Module 4), which is the process by which digital evidence of crimes and cybercrimes is collected, acquired, preserved, analysed, interpreted, reported, and presented during legal proceedings.

Learning outcomes

L1 Identify, analyse, and critically assess legal and ethical obligations of cybercrime investigators and digital forensics professionals
L2 Identify essential phases in the digital forensics process
L3 Articulate and critically evaluate the ways in which digital evidence is identified, collected, acquired, and preserved
L4 Discuss and appraise the processes involved in digital evidence analysis and the reporting of findings based on this analysis
L5 Explain and apply a framework for assessing the admissibility of digital evidence in courts

Assessment of student learning

Learning Outcomes	Bloom's Taxonomy (Original/Revised)	Assessment Tools
L1	Knowledge/Remembering Comprehension/Understanding Analysing Evaluating	Homework #3; Homework #4; Review Questions; Class Discussions
L2	Knowledge/Remembering Comprehension/Understanding	Review Questions; Class Discussions
L3	Knowledge/Remembering Comprehension/Understanding Applying Analysing Evaluating	Exercise #1; Exercise #2; Review Questions; Class Discussions
L4	Knowledge/Remembering Comprehension/Understanding Analysing Evaluating	Exercise #3; Homework #1; Review Questions; Class Discussions

L5	Comprehension/Understanding Applying Analysing	Homework #2; Review Questions; Class Discussions

Module 7: International Cooperation against Cybercrime

Cybercrime can be perpetrated by offenders anywhere in the world with an Internet connection. The adverse impacts of cybercrime can be experienced outside of the country in which the perpetrator resides. The transnational nature of this crime challenges traditional notions of jurisdiction and requires cooperation of criminal justice agents across the globe (see also the E4J University Module Series on Organized Crime, particularly Module 11 on International Cooperation to Combat Transnational Organized Crime). This cooperation has been observed, for example, in international investigations of online illicit markets (or dark markets), such as Darkode (i.e., a dark market known for selling illicit goods and services, including access to stolen data and malware). Coordinated efforts between law enforcement authorities from 20 countries led to the identification, arrest, and search of members and associates of this site (US Department of Justice, 2015). Despite this and other successful cooperative efforts between countries, barriers to international cooperation against cybercrime still exist today. This Module explores the notions of sovereignty and jurisdiction relating to cybercrime, international cooperation mechanisms, and the challenges to international cooperation.

Learning outcomes

L1 Describe and differentiate between sovereignty and jurisdiction, and apply them to cybercrime
L2 Compare, contrast, and appraise various formal international cooperation mechanisms
L3 Evaluate informal international cooperation mechanisms
L4 Discuss and compare data retention, preservation, and access practices between countries
L5 Identify and assess challenges relating to extraterritorial evidence
L6 Discuss the deficit in national capacity to conduct cybercrime investigations and its impact on international cooperation

Assessment of student learning

Learning Outcomes	Bloom's Taxonomy (Original/Revised)	Assessment Tools

L1	Comprehension/Understanding Analysing	Exercise #1; Review Questions; Class Discussions
L2	Knowledge/Remembering Comprehension/Understanding Analysing Evaluating	Exercise #2; Homework #1; Homework #2; Review Questions; Class Discussions
L3	Knowledge/Remembering Comprehension/Understanding Evaluating	Homework #1; Homework #2; Review Questions; Class Discussions
L4	Knowledge/Remembering Comprehension/Understanding Evaluating	Exercise #3; Review Questions; Class Discussions
L5	Knowledge/Remembering Comprehension/Understanding Evaluating	Homework #2; Review Questions; Class Discussions
L6	Knowledge/Remembering Comprehension/Understanding Analysing Evaluating	Homework #2; Review Questions; Class Discussions

Module 8: Cybersecurity and Cybercrime Prevention: Strategies, Policies and Programmes

Information and communication technology (ICT) is integral to national and global development by facilitating innovation and economic growth. The ever-increasing interdependency of digital devices within countries, as well as growing network connections with the digital systems of other countries, has made ICT vulnerable to cybercrime. Because cybercrime can adversely impact national security, international security, and the global economy, the protection of ICT is considered of paramount importance nationally and internationally. In view of that, countries worldwide have published strategies delineating how ICT will be protected from cybercrime and cybercriminals. Module 8 critically examines these strategies, and the tools used to assess these strategies and countries' cyber-related security and crime prevention efforts.

Learning outcomes

L1 Discuss Internet governance and identify and assess Internet principles, conflicts that arise in the realization of these principles, and barriers to universal Internet governance

L2 Describe the basic features of cybersecurity strategies and differentiate between cybersecurity and cybercrime prevention strategies
L3 Explain and evaluate the objectives and lifecycle of national cybersecurity strategies
L4 Identify, examine, and evaluate frameworks for international cooperation on cybersecurity matters
L5 Assess national and international efforts to enhance countries' cybersecurity posture

Assessment of student learning

Learning Outcomes	Bloom's Taxonomy (Original/Revised)	Assessment Tools
L1	Knowledge/Remembering Comprehension/Understanding Evaluating	Exercise #1; Homework #1; Review Questions; Class Discussions
L2	Knowledge/Remembering Comprehension/Understanding Analysing Evaluating	Exercise #2; Review Questions; Class Discussions
L3	Applying Analysing Evaluating	Review Questions; Class Discussions
L4	Comprehension/Understanding Applying Analysing Evaluating	Exercise #3; Review Questions; Class Discussions
L5	Evaluating	Homework #2; Review Questions; Class Discussions

Module 9: Cybersecurity and Cybercrime Prevention: Practical Applications and Measures

Cybersecurity refers to the strategies, policies, guidelines, procedures, practices, and measures that are designed to identify threats and vulnerabilities, prevent threats from exploiting vulnerabilities, mitigate the harm caused by materialized threats, and safeguard people, property, and information. Building on Cybercrime Module 8 on Cybersecurity and Cybercrime Prevention: Strategies, Policies, and Programmes, Module 9 covers the practical aspects of cybersecurity and cybercrime prevention, including risk assessments and the measures used to prevent, detect, respond to and recover from cybersecurity incidents.

Learning outcomes

L1 Define, discuss, and evaluate assets, threats, vulnerabilities, and risks
L2 Identify and assess the ways in which vulnerabilities can be disclosed
L3 Describe and critique the relationship between cybersecurity and usability
L4 Discuss situational crime prevention and apply it cybercrime prevention and reduction
L5 Discuss and analyse incident detection, response and recovery

Assessment of student learning

Learning Outcomes	Bloom's Taxonomy (Original/Revised)	Assessment Tools
L1	Knowledge/Remembering Comprehension/Understanding Evaluating	Review Questions; Class Discussions
L2	Comprehension/Understanding Evaluating	Exercise #1; Homework #1; Homework #2; Review Questions; Class Discussions
L3	Knowledge/Remembering Comprehension/Understanding Analysing Evaluating	Homework #3; Review Questions; Class Discussions
L4	Comprehension/Understanding Applying Synthesis/Creating	Exercise #2; Review Questions; Class Discussions
L5	Comprehension/Understanding Analysing	Exercise #3; Case Study; Review Questions; Class Discussions

Module 10: Privacy and Data Protection

Personal data is sought by both criminals and cybercriminals and used in the commission of crime and cybercrime. This personal data can be obtained from a variety of sources (these sources are discussed in Cybercrime Module 4 on Introduction to Digital Forensics). This personal data can reveal information about individuals' age, race, ethnicity, nationality, gender, religious and political beliefs, sexual orientation, thoughts, preferences, hobbies, medical history and concerns, psychological disorders, profession, employment status, military service, affiliations, relationships, geolocation, habits, routines, and other activities, among

other information (see Cybercrime Module 4 on Introduction to Digital Forensics). This personal data, when aggregated, can provide an almost complete picture of individuals' personal and professional lives.

Module 10 critically examines the impact of data aggregation, as well as the impact of data collection, storage, analysis, use, and sharing, on privacy and security. Specifically, this Module covers privacy as a human right, the relationship between privacy and security, the ways in which cybercrime compromises privacy and data security, and data protection and breach notification laws, as well as the ways in which data is (and can be) protected to secure persons, property, and information.

Learning outcomes

L1 Discuss privacy and its importance as a human right
L2 Identify and analyse the impact of cybercrime on privacy
L3 Critically evaluate the relationship between security and privacy
L4 Critique data protection and breach notification laws and practices across nations
L5 Critically assess data protection enforcement practices of states and recommend effective ways to protect data

Assessment of student learning

Learning Outcomes	Bloom's Taxonomy (Original/Revised)	Assessment Tools
L1	Comprehension/Understanding	Exercise #3; Review Questions; Class Discussions
L2	Comprehension/Understanding Analysing	Exercise #1; Review Questions; Class Discussions
L3	Evaluating	Exercise #1; Homework #1; Review Questions; Class Discussions
L4	Evaluating	Exercise #1; Exercise #2; Homework #2; Review Questions; Class Discussions
L5	Synthesis/Creating	Exercise #2; Review Questions; Class Discussions

Module 11: Cyber-Enabled Intellectual Property Crime

The Internet and Internet-enabled digital devices are force multipliers for intellectual property crime because they enable intellectual property to be uploaded, copied, downloaded, and shared instantly worldwide. International and regional cooperation on intellectual property crime and protection matters are critical. This cooperation can (and has) involve implementing national, regional, and international property laws, and developing national capacity to protect intellectual property and prevent intellectual property crime online and offline. Ultimately, intellectual property crime denies creators and innovators and those who make intellectual property available their economic returns on their creations, innovations, unique identifiers, and/or undisclosed information.

Module 11 examines intellectual property and its cyber-enabled unauthorized access, distribution, and use. Specifically, this Module examines what intellectual property is, types of intellectual property, the causes, reasons, and perceived justifications for cyber-enabled copyright and trademark offences, and protective and preventive measures against such offences.

Learning outcomes

L1 Discuss intellectual property and the importance of its protection
L2 Differentiate between various forms of intellectual property
L3 Critically evaluate national, regional, and international laws and treaties relating to intellectual property protection
L4 Identify and discuss various criminological, sociological, psychological, and economic theories and critically assess their applicability to cyber-enabled copyright and trademark offences
L5 Critically evaluate national, regional, and international intellectual property protection and prevention efforts

Assessment of student learning

Learning Outcomes	Bloom's Taxonomy (Original/Revised)	Assessment Tools
L1	Comprehension/Understanding	Exercise #3; Exercise #4; Homework #3; Review Questions; Class Discussions

L2	Analysing	Homework #2; Exercise #3; Exercise #3; Review Questions; Class Discussions
L3	Evaluating	Homework #2; Homework #3; Review Questions; Class Discussions
L4	Knowledge/Remembering Comprehension/Understanding Evaluating	Exercise #1; Homework #1; Review Questions; Class Discussions
L5	Evaluating	Exercise #1; Exercise #2; Exercise #4

Module 12: Interpersonal Cybercrime

Information and communications technology (ICT) provides innumerable opportunities for participation in civic and political affairs and social activities and has the potential to provide individuals with access to education and economic prospects, irrespective of their geographic location. ICT also provides users with immeasurable opportunities to communicate with others and share information. These opportunities, however, can be misused by others to sexually exploit and abuse children and adults, perpetrate anti-social and aggressive acts, and incite violence and other forms of aggression at individuals, groups and/or targeted populations to cause harm to others. Module 12 explores some of these cybercrimes, looking in particular at child sexual exploitation and abuse, cyberstalking, cyberharassment, cyberbullying, various forms of gendered cybercrimes (e.g., image-based sexual abuse and sextortion), and the measures used to counter, combat, and prevent these cybercrimes.

Learning outcomes

L1 Define interpersonal cybercrime
L2 Define and differentiate between types of interpersonal cybercrime
L3 Describe and analyse the ways in which information and communication technology is used to facilitate these types of interpersonal cybercrime
L4 Identify and critically engage with the role of law in addressing these cybercrimes
L5 Recognize and assess the obstacles to preventing and responding to various interpersonal cybercrimes

Assessment of student learning

Learning Outcomes	Bloom's Taxonomy (Original/Revised)	Assessment Tools
L1	Knowledge/Remembering	Review Questions; Class Discussions
L2	Knowledge/Remembering Comprehension/Understanding Analysing	Exercise #2; Homework #4; Review Questions; Class Discussions
L3	Comprehension/Understanding Analysing	Exercise #1; Homework #1; Homework #3; Homework #4; Review Questions; Class Discussions
L4	Comprehension/Understanding Evaluating	Homework #2; Review Questions; Class Discussions
L5	Comprehension/Understanding Evaluating	Exercise #1; Exercise #3; Exercise #4; Homework #4; Review Questions; Class Discussions

Module 13: Cyber Organized Crime

The Internet provides criminals with access to victims and customers anywhere in the world with an Internet connection. These criminals take advantage of the ease with which information, communications, and money traverses cyberspace. They utilize the Internet to share knowledge and communicate undetected, sell stolen data, goods, and services, launder illicitly acquired money, as well as exchange cybercrime tactics and tools used to commit cybercrimes These criminals can operate alone or in different types of organized criminal groups. Module 13 examines the types of crimes that are considered as cyber organized crime and the types of organized criminal groups that engage in cybercrime. This Module further explores the measures used to counter cyber organized crime.

Learning outcomes

L1 Describe cyber organized crime and criminal groups that engage in cyber organized crime
L2 Identify and discuss the structures and characteristics of organized criminal groups that engage in cyber organized crime
L3 Examine different types of cyber organized crime

L4 Explain and analyse the ways in which information and communication technology is used to commit cyber organized crime
L5 Critically evaluate the measures used to counter cyber organized crime

Assessment of student learning

Learning Outcomes	Bloom's Taxonomy (Original/Revised)	Assessment Tools
L1	Knowledge/Remembering Comprehension/Understanding	Exercise #1; Review Questions; Class Discussions
L2	Knowledge/Remembering Comprehension/Understanding	Exercise #1; Review Questions; Class Discussions
L3	Knowledge/Remembering Comprehension/Understanding Analysing	Review Questions; Class Discussions
L4	Comprehension/Understanding Applying Analysing	Exercise #3; Homework #1; Review Questions; Class Discussions
L5	Evaluating	Exercise #2; Homework #2; Homework #3; Homework #4; Review Questions; Class Discussions

Module 14: Hacktivism, Terrorism, Espionage, Disinformation Campaigns, and Warfare in Cyberspace

Module 14 of the E4J University Module Series on Cybercrime examines topics such as hacktivism, terrorism, espionage, disinformation campaigns, and warfare in cyberspace, as well as national and international perspectives and responses to these cyber activities. The purpose of this Module is to discuss these topics and identify current debates and conflicting views on these topics within and between countries.

Learning outcomes

L1 Critically examine hacktivism, cyberespionage, cyberterrorism, cyberwarfare, information warfare, disinformation, and electoral fraud
L2 Critically discuss and analyse the legal frameworks governing these activities
L3 Critically assess the lawfulness of responses to these activities
L4 Propose lawful responses to some of these activities

Assessment of student learning

Learning Outcomes	Bloom's Taxonomy (Original/Revised)	Assessment Tools
L1	Analysing	Exercise #1; Exercise #2; Exercise #4; Homework #1; Homework #2; Review Questions; Class Discussions
L2	Knowledge/Remembering Comprehension/Understanding Analysing	Exercise #1; Exercise #2; Homework #1; Homework #2; Homework #3; Review Questions; Class Discussions
L3	Evaluating	Exercise #3; Homework #2; Homework #3; Review Questions; Class Discussions
L4	Synthesis/Creating	Exercise #3; Exercise #4; Homework #4; Class Discussions

Conclusion

The E4J initiative offers an innovative approach to cybercrime education at all three levels of education, an area that is of critical importance to address the current worldwide deficit in national cybercrime prevention and cybersecurity capacity. It is the hope of the United Nations Office on Drugs and Crime that universities around the world will make use of this E4J University Module Series on Cybercrime and that it adds value to new or existing course offerings, for both students and lecturers.

References

Anderson, Lorin W. and David R. Krathwohl. (2001). *A Taxonomy for Learning, Teaching and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives*, Complete Edition. Longman.

Berkeley Center for Teaching & Learning, Active Learning Strategies, https://teaching.berkeley.edu/active-learning-strategies.

Bloom, Benjamin S. (1956). *Taxonomy of educational objectives* Book 1: Cognitive domain. Addison-Wesley Longman.

Brown, Peter, Mark McDaniel, and Henry L. Roediger. (2014). *Make It Stick: The Science of Successful Learning*. Harvard University Press.

Center for Advanced Research on Language Acquisition (CARLA) (n.d.). Continuous Improvement: Objectivity and Subjectivity in Evaluation. University of Minnesota. http://carla.umn.edu/assessment/vac/improvement/p_6.html.

Schwartz, Michelle. (n.d.). Matching Assessments to Learning Outcomes Ryerson University, Learning & Teaching Office. https://www.ryerson.ca/content/dam/lt/resources/handouts/examslearningoutcomes.pdf

Segal, Mark (2013). *How To Train: A Practical Guide for Training and Working with Others* https://marksegaldotnet.files.wordpress.com/2011/07/howtotrain-marksegal3.pdf.

Yale Poorvu Center for Teaching and Learning, Active Learning, https://poorvucenter.yale.edu/ActiveLearning.

Acknowledgements

This Teaching Guide and the associated University Module Series on Cybercrime were developed by the United Nations Office on Drugs and Crime (UNODC) under its Education for Justice (E4J) initiative and in line with its Global Programme for the Implementation of the Doha Declaration.

UNODC wishes to thank Ms. Marie-Helen Maras of the City University of New York John Jay College of Criminal Justice for her leading role in drafting this Guide and the associated Modules. UNODC would furthermore like to thank Mr. Joshua James of Hallym University, Republic of Korea for his contribution to this Guide and the associated Modules.

UNODC furthermore acknowledges with profound gratitude those who have supported the development of the Modules and the Teaching Guide by reviewing early drafts and participating in the E4J Expert Group Meetings in August and November 2018, including several academic experts unable to participate in the Expert Workshops in person (in alphabetical order):

Mr. Nikolay Akatyev (Horangi Cyber Security)
Mr. Albert Antwi-Boasiako (Kwame Nkrumah University of Science and Technology, Ghana)
Mr. Vladimir Aras (Federal Prosecutor, Federal University of Bahia, Brazil)
Mr. Angel Jr Averia (Philippine Computer Emergency Response Team)
Mr. Roderic Broadhurst (Australian National University)
Mr. Robin Bryant (Canterbury Christ Church University, United Kingdom)
Mr. Lennon Chang (Monash University, Australia)
Mr. Yannick Chatelain (Grenoble School of Management, France)
Mr. Pavan Duggal (Supreme Court of India)
Ms. Myriam Dunn Cavelty (Swiss Federal Institute of Technology)
Ms. Asher Flynn (Monash University, Australia)
Mr. Zhixiong Huang (Wuhan University, China)
Ms. Laura Huey (University of Western Ontario, Canada)
Mr. Abhaya Induruwa (Canterbury Christ Church University, United Kingdom)
Ms. Bahija Jamal (Hassan II University, Morocco)
Mr. Oleksandr Komarov (Yaroslav Mudryi National Law University, Ukraine)
Mr. Edwin Kruisbergen (Ministry of Justice and Security, The Netherlands)
Mr. Alexander Kukhianidze (Tbilisi State University, Georgia)
Mr. Chat Le Nguyen (Fiji National University)
Mr. Asaf Lubin (Yale College, United States of America)
Mr. Stephen Mason (United Kingdom)

Mr. Milos Mijomanovic (INTERPOL)
Mr. Brian Nussbaum (University at Albany, United States of America)
Mr. Adedeji Oyenuga (Lagos State University, Nigeria)
Mr. Sergey Petrenko (Innopolis University, Russian Federation)
Mr. Nigel Phair (University of Canberra, Australia)
Mr. James Popham (Wilfrid Laurier University, Canada)
Ms. Pauline Reich (Nanyang Technological University, Singapore)
Mr. Nodirbek Salaev (Tashkent State University of Law, Uzbekistan)
Mr. Yun Shen (Symantec Research Labs)
Mr. Ahmed Shosha (Nile University, Egypt)
Mr. Vaclav Stupka (Masaryk University, Czech Republic)
Mr. Nedko Tagarev (University of National and World Economy, Bulgaria)
Mr. Hamed Tofangsaz (University of Waikato, New Zealand)
Ms. Bermet Tursunkulova (American University of Central Asia, Kyrgyz Republic)
Mr. Ian Walden (Queen Mary, University of London, United Kingdom)
Mr. David Wall (University of Leeds, United Kingdom)
Ms. Elena Yi (Yaroslav Mudryi National Law University, Ukraine)

UNODC also thanks colleagues from the Office of the United Nations High Commissioner for Human Rights, and especially Mr. Tim Engelhardt.

UNODC also acknowledges the contributions of the following UNODC staff, who were responsible for developing this Guide and the associated Modules: Ms. Kamola Ibragimova, Mr. Patrick Boismenu, Mr. Neil J. Walsh, Mr. Marco Teixeira, Ms. Julia Pilgrim, Ms. Bianca Kopp. The following UNODC staff and personnel also made valuable contributions: Mr. Oleksiy Feshchenko, Ms. Malin Oestevik, Mrs. Nayelly Loya Marin, Ms. Wendy O'Brien, Ms. Alexandra Martins, Ms. Riikka Puttonen, Mr. Dimosthenis Chrysikos, Ms. Flavia Romiti, Ms. Jenna Dawson-Faber, Mr. Arturo Laurent, Mr. Joaquin Zuckerberg.

Appendix A: Glossary of Terms

This glossary includes the terms discussed in the 14 Cybercrime Modules.

Access controls. Measures that establish privileges, determine authorized access, and prevent unauthorized access.

Active digital footprint. Created by data provided by the user.

Advanced fee fraud. A computer-related fraud involving a request for an advance fee to complete a transfer, deposit or other transaction in exchange for a larger sum of money.

Advanced persistent threats. Individuals and/or groups that persistently target an entity. Also known as *APTs*.

Appellations of origin. Symbols of products quality and the reputation of the place of its creation property, which cannot be used unless the product was developed in that region according to standards of practice. Also known as *geographical indications*.

Anonymity. The shielding of one's identity to enable individuals to engage in activities without revealing themselves and/or their actions to others.

Anonymizers. These proxy servers enable users to hide identity data by masking their IP address and substituting it with a different IP address. Also known as *anonymous proxy servers*.

Anonymous proxy servers. These proxy servers enable users to hide identity data by masking their IP address and substituting it with a different IP address. Also known as *anonymizers*.

Anti-digital forensics. Tools and techniques used to obfuscate cybercrime investigation and digital forensics efforts. Also known as *antiforensics*.

Antiforensics. Tools and techniques used to obfuscate cybercrime investigation and digital forensics efforts. Also known as *anti-digital forensics*.

Application and file analysis. Type of analysis that is performed to examine applications and files on a computer system to determine the perpetrator's knowledge of and intent and capabilities to commit cybercrime.

Asset. Something that is considered important and/or valuable.

Attribution. The determination of who and/or what is responsible for a cybercrime.

Availability. Data, services, and systems are accessible on demand.

Backdoor. A secret portal used to gain unauthorized access to systems.

Best evidence. The original piece of evidence or an accurate duplicate of the original.

Big data. Large volumes of structured and unstructured data that can be consolidated and analysed to reveal information about associations, patterns, and trends.

Brute force attack. The use of a script or bot to guess user credentials.

Back-tracing. The process of tracing illicit acts back to the source of the cybercrime. Also known as traceback.

Botcode. A type of malicious software that enables the remote control of these devices and use them to commit cybercrimes, steal information, and/or engage in cyberattacks.

Botherder. Controller of bot-infected digital devices.

Botnet. A network of computers infected with botcode.

Bulletproof hosting. A service that enables criminals to utilize servers to commit cybercrime, store illicit content, and protect illicit content from being accessed by law enforcement authorities and/or being taken offline.

Business continuity plan. Outlines instructions to be followed and actions to be taken in the event of a cybersecurity incident. Also known as *emergency management plan*.

Catphishing. False or misleading promises of love and companionship designed to scam individuals out of their time, money and/or other items.

Censorship. The prohibition of information, visual depictions, and written or oral communications that are prohibited by law and/or their suppression by a government, community or group because they are unlawful and/or viewed as harmful, unpopular, undesirable, or politically incorrect.

Chain of custody. A detailed log about the evidence, the condition of the evidence, its collection, storage, access, and transfer and reasons for its access and transfer, is essential to ensure the admissibility of digital evidence in most courts of law.

Child grooming. Enticement of children or solicitation of children for sexual purposes.

Child sex trafficking. Acting in some manner that recruits, leads, causes, maintains, and/or otherwise facilitates the commercial sexual exploitation of children.

Child sexual abuse material. The representation of child sexual abuse and/or other sexualized acts using children.

Child sexual abuse to order. Viewers of child sexual abuse can be actively involved in abuse by communicating with the child, the sexual abuser, and/or facilitator of the child sexual abuse and requesting specific physical acts and/or sexual acts to be performed on and/or performed by the child.

Circumstantial evidence. Evidence that infers the truth of a matter.

Clearnet. Indexed websites that are accessible and available to the public and can be searched using traditional search engines. Also known as *Surface Web* or *Visible Web*.

Code of ethics. Guidelines covering right and wrong conduct to inform decision-making.

Commercial sexual exploitation of children. A term used to describe a range of activities and crimes that involve the sexual abuse of children for some kind of remuneration of any monetary or non-monetary value.

Computer data. Any form of representation of information that is processed by a system of a digital device. Also known as *computer information* or *data*.

Computer Emergency Response Team. A team that provides support for cybersecurity incidents. Also known as *Computer Security Incident Response Team*.

Computer information. Any form of representation of information that is processed by a system of a digital device. Also known as *computer data* or *data*.

Computer network. Two or more computers that send and receive data between them.

Computer Security Incident Response Team. A team that provides support for cybersecurity incidents. Also known as *Computer Emergency Response Team.*

Computer system. A stand-alone or networked device that performs data processing among other functions.

Confidentiality. Systems, networks, and data are protected, and only authorized users can access them.

Confirmation bias. The process whereby individuals look for and support results that support their working hypothesis and dismiss results that conflict with their working hypothesis.

Content data. Words in written communications or spoken words.

Coordinated vulnerability disclosure. The practice of harmonized information sharing and disclosure of vulnerabilities to relevant stakeholders along with the tactics used for its mitigation.

Copyrights. Creative products, such as artistic and literary works, protected by law.

Crime displacement. When a crime that was intended for one target is committed on another target because of security measures in place.

Crime reconstruction. This process seeks to determine *who* was responsible for the crime, *what* happened, *where* did the crime occur, *when* did the crime take place, and *how* the crime unfolded, through the identification, collation, and linkage of data. Also known as *event reconstruction*.

Critical infrastructure. Designated essential sectors that are considered fundamental to the proper functioning of society.

Cryptocurrency. A form of digital currency secured utilizing advanced encryption.

Crytopjacking. A tactic whereby the processing power of infected computers is used to mine cryptocurrency for the financial benefit of the person (or persons) controlling the bot-infected digital devices.

Cyber-dependent crime. A cybercrime that would not be possible without the Internet and digital technologies.

Cyber-enabled crimes. A cybercrime facilitated by the Internet and digital technologies.

Cyber organized crime. A term used to describe a continuing criminal enterprise that rationally works to profit from illicit activities that are in demand online.

Cyber organized criminals. A structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with the United Nations Convention against Transnational Organized Crime of 2000, which operate in whole or in part online, in order to obtain, directly or indirectly, a financial or other material benefit.

Cyber proxies. The use of intermediaries to directly or indirectly contribute to a cyber-dependent crime intentionally targeting a state.

Cryptomarkets. A website utilizing cryptography to protect users of the site.

Cyberbullying. The use of information and communication technology by children to annoy, humiliate, insult, offend, harass, alarm, stalk, abuse or otherwise attack another child or children.

Cyberespionage. The use of information and communication technology by government actors, state-sponsored or state-directed groups, or others acting on behalf of a government, to gain unauthorized access to systems and data in an effort to collect intelligence on their targets in order to enhance their own country's national security, economic competitiveness, and/or military strength.

Cyberharassment. The use of information and communication technology to intentionally humiliate, annoy, attack, threaten, alarm, offend and/or verbally abuse an individual (or individuals).

Cryptoransomware. Malware that infects a user's digital device, encrypts the user's documents, and threatens to delete files and data if the victim does not pay the ransom.

Cybersmearing. Posting or otherwise distributing of false information or rumours about an adult or child to damage the victim's social standing, interpersonal relationships, and/or reputation.

Cyberspace. An environment accessed by Internet-enabled digital technology within which online activities take place.

Cyberstalking. The use of information and communication technology to commit a series of acts over a period of time designed to harass, annoy, attack, threaten, frighten, and/or verbally abuse an individual (or individuals).

Cybersecurity. The collection of strategies, frameworks, and measures that are designed to identify threats and vulnerabilities of systems, networks, services, and data to these threats; prevent the exploitation of vulnerabilities; mitigate the harm caused by materialized threats; and safeguard people, property, and information and communication technology.

Cybersecurity posture. A term used to describe the cybersecurity capabilities of a country, organization or business.

Cyberterrorism. The cyber-dependent crimes perpetrated against critical infrastructure to cause some form of harm and to provoke fear in the target population.

Cyberwarfare. Cyber acts that compromise and disrupt critical infrastructure systems, which amount to an armed attack

Dark Web. The part of the World Wide Web, which is known for its obscure and hidden websites that host illicit activities, goods, and services, and can only be accessed using specialized software. Also known as darknet.

Darknet. The part of the World Wide Web, which is known for its obscure and hidden websites that host illicit activities, goods, and services, and can only be accessed using specialized software. Also known as Dark Web.

Data. Any form of representation of information that is processed by a system of a digital device. Also known as *computer data* or *computer information*.

Data hiding analysis. Type of analysis that searches for hidden data on a system.

Data preservation. Requests are made to service providers by law enforcement in an effort to retain data before it is deleted or altered in any way.

Data mining. The retrieval of information from data sets.

Data protection. The safeguarding of personal information and regulates its collection, storage, analysis, use, and sharing.

Data protection by design. Privacy measures embedded in the design of systems and technologies. Also known as *privacy by design.*

DDoS attack. The use of multiple computers and other digital technologies to conduct coordinated attacks with the intention of overwhelming servers to prevent legitimate users' access. Also known as a *distributed denial of service attack.*

Deep Web. The part of the World Wide Web that is not indexed by search engines and is not easily accessible and/or available to the public.

Denial of service attack. A cybercrime that interferes with systems by overwhelming servers with requests to prevent legitimate traffic from accessing a site and/or using a system. Also known as DoS attack.

Design patents. A form of intellectual property that includes designs that are created with the specific purpose of being aesthetically pleasing to consumers and impacts their choice between products. Also known as *industrial designs*.

Deterrence. Discouraging illicit activity through punishment.

Digital evidence. Data obtained from information and communication technology. Also known as *electronic evidence*.

Digital footprint. Data left behind by ICT users that can reveal information about them, including age, gender, race, ethnicity, nationality, sexual orientation, thoughts, preferences, habits, hobbies, medical history and concerns, psychological disorders, employment status, affiliations, relationships, geolocation, routines, and other activities.

Digital forensic process. The search, retrieval, preservation, and maintenance of digital evidence; description, explanation and establishment of the origin of digital evidence and its significance; the analysis of evidence and its validity, reliability and relevance to the case; and the reporting of evidence pertinent to the case.

Digital forensics. A branch of forensic science that applies matters of law to information and communication technology and digital evidence.

Digital piracy. The illegal download of a movie from a third-party website that does not have the right to distribute the copyrighted work.

Direct evidence. Evidence that establishes a fact.

Disinformation. The deliberate spreading of false information.

Disinhibition. The process whereby an individual demonstrates a lack of social restraint with regards to online behaviour.

Dissociative anonymity. Individuals detachment of their online behaviour from their offline behaviour due to the anonymity afforded to them when utilizing the Internet and digital technology.

Dissociative imagination. Individuals' view of cyberspace as a forum within which the rules of everyday interactions, codes of conduct, social norms, and/or laws do not apply, disinhibiting the individual to act in a manner contrary to offline rules of everyday interactions, codes of conduct, social norms, and/or laws.

Distributed denial of service attack. The use of multiple computers and other digital technologies to conduct coordinated attacks with the intention of overwhelming servers to prevent legitimate users' access. Also known as a DDoS attack.

Dogpiling. A tactic whereby users within an online space bombard victims with offensive, insulting, and threatening messages to silence the target, force them to take back what they said and/or apologize, or to force them to leave the platform.

Domain name. A representation of an IP address in an Internet (or web) browser.

Domain Name System. Enables Internet access by translating domain names to IP address.

DoS attack. A cybercrime that interferes with systems by overwhelming servers with requests to prevent legitimate traffic from accessing a site and/or using a system. Also known as *denial of service attack.*

Doxing. Personal information about individuals posted online to cause the individual some form of harm.

Doxware. A form cryptoransomware that perpetrators use against victims that releases the user's data if ransom is not paid to decrypt the files and data.

Dual criminality. A clause in treaties requiring acts to be considered illegal in cooperating countries.

eDiscovery. The process of searching, identifying, and preserving digital data for use as evidence in a legal proceeding.

Electoral fraud. The use of unlawful tactics to influence elections.

Electronic evidence. Data obtained from information and communication technology. Also known as *digital evidence*.

Emergency management plan. Outlines instructions to be followed and actions to be taken in the event of a cybersecurity incident. Also known as *business continuity plan*.

Encryption. Measure that blocks third party access to users' information and communications.

Event reconstruction. This process seeks to determine *who* was responsible for the event, *what* happened, *where* did the event occur, *when* did the event take place, and *how* the event unfolded, through the identification, collation, and linkage of data. Also known as *crime reconstruction*.

Expected utility theory. A theory that holds that people engage in actions when the expected utility from these actions are higher than the expected utility of engaging in other actions.

Fake news. Propaganda and disinformation masquerading as real news.

Fifth domain. A term used to describe cyberspace as another domain of warfare.

Firewall. A security measure that restricts the free flow of information by blocking unauthorized traffic data.

Forensic relevance. The relevance of forensic data is determined by whether the digital evidence: links or rules out a connection between the perpetrator and the target and/or the crime scene; supports or refutes perpetrator, victim and/or witness testimony; identifies the perpetrator(s) of the cybercrime; provides investigate leads; provides information about the method of operation of the perpetrator; and shows that a crime has taken place.

File carving. Search based on content identifiers.

First responders. Individuals who respond first to the scene and are responsible for securing evidence at the scene.

Full vulnerability disclosure. Publicly publishing the software or hardware vulnerability through online forums and websites before a fix is available.

Functional analysis. The assessment of the performance and capabilities of systems and devices involved in events.

General deterrence. Punishment designed to send the message to others that similar illicit behaviour will receive similar severe punishment.

Geographical indications. Symbols of products quality and the reputation of the place of its creation property, which cannot be used unless the product was developed in that region according to standards of practice. Also known as *appellations of origin.*

Hacking. Unauthorized access to systems, networks, and data.

Hard drive. An internal, persistent memory in a computer.
Hearsay. Out of court statements.

Hash. A generated value.

Human flesh search engine. A term used to describe online users work together to identify a target and perpetrate coordinated online abuse against the target.

Identity management. The process of authenticating users' identities, identifying associated privileges, and granting user access based on these privileges.

Identity-related crime. A perpetrator unlawfully assumes and/or misappropriates the identity of the victim and/or uses the identity and/or information associated with the identity for illicit purposes.

Image-based sexual abuse. A form of sexual violence whereby sexually explicit images and/or videos of the victims are intentionally created, distributed or threatened to be distributed without the consent of the victims. This may be to cause some form of harm to the victim and/or to benefit the perpetrator in some way (e.g. monetary gain, sexual gratification, social status building and more).

Imaging. Creating a duplicate copy of the content of the digital device.

Incident detection. The process of identifying threats by actively monitoring assets and finding anomalous activity.

Industrial control systems. Systems that command and control critical infrastructure processes.

Industrial designs. A form of intellectual property that includes designs that are created with the specific purpose of being aesthetically pleasing to consumers and impacts their choice between products. Also known as *design patents*.

Information warfare. The collection, distribution, modification, disruption, interference with, corruption, and degradation of information to gain some advantage over an adversary.

Inoculation theory. This theory holds that the way to inoculate individuals from persuasion attempts of others is to expose them to these attempts and given them tools they need to resist these attempts.

Integrity. Data is accurate and trustworthy and has not been modified.

Intellectual property. Products of creativity, such as works, innovations, creations, original expression of ideas, and secret business practices and processes, that individuals have rights to as prescribed by law.

Internet governance. The creation and application of Internet principles, rules, and procedures by various stakeholders to guide the use of the Internet and shape its development.

Internet of Things. An interconnected and interoperable network of Internet-enabled devices that facilitate the monitoring of objects, plants, animals, and people, and the collection, storage, examination, and dissemination of information about them.

Internet penetration rate. The portion of the population in an area that uses the Internet.

Internet Protocol address. A unique identifier assigned by an Internet service provider to an Internet-connected digital device to connect to the Internet. Also known as *IP address*.

Internet service provider. Provides Internet services to a computer system or a system of another digital device.

Internet trolls. Individuals that purposely post rude, aggressive, and offensive remarks designed to create discord and discontent online.

IP address. A unique identifier assigned by an Internet service provider to an Internet-connected digital device to connect to the Internet. Also known as *Internet Protocol address*.

Interpersonal cybercrime. Cybercrimes committed by individuals against other individuals with whom they are interacting, communicating, and/or having some form of real or imagined relationship.

Intrusion detection systems. A cybersecurity measure that enables the detection of cyberattacks and unauthorized access and use of systems, networks, data, services, and related resources.

Jurisdiction. A state's power and authority to enforce laws and punish non-compliance with laws.

Key performance indicators. Measures that are used to determine progress towards the realization of the strategic objectives of the national cybersecurity strategy.

Letters rogatory. Written requests from national courts for evidence from a foreign country.

Live streaming of child sexual abuse. The real-time broadcasting of child sexual abuse to viewers (often) in remote locations.

Logical extraction. The search for and acquisition of evidence from the file system location.

Keyword searches. Search based on terms provided by the investigator.

Knowledge management. The process of identification and assessment of knowledge needs and the utilization of knowledge assets.

Malware. Malicious software.

Metadata. Data about the content. Also known as *non-content data*.

Microlaundering. A form of money-laundering whereby the perpetrators launder a significant amount of money through multiple small transactions.

Misinformation. False or inaccurate information.

Money-laundering. The concealment of illicit proceeds through a combination of legitimate and illegitimate transactions.

Money mules. Individuals who either knowingly or unknowingly commit crimes and/or cybercrimes by obtaining and transferring illicit goods, engaging in illicit services, and/or illegally receiving or transferring money for others for remuneration.

Morphing. A victim's face or head superimposed on the bodies of others for the purpose of defamation, pornography, and/or sexual abuse.

Mutual legal assistance treaty. An agreement between countries to cooperate on investigations and prosecutions of certain and/or all offences proscribed by both parties under national law.

Net neutrality. Requires all data, irrespective of source, to be treated equally.

Neutralization techniques. Techniques used to overcome or minimize negative emotions associated with the engagement in illicit activity.

Non-content data. Data about the content. Also known as *metadata*.

Online child sexual abuse. The use of information and communication technology as a *means* to sexually abuse children

Online child sexual exploitation. The use of information and communication technology as a *means* to sexually exploit children, where child sexual abuse and/or other sexualized acts using children involve an exchange of some kind.

Online impersonation. The impersonation of victims by creating accounts with similar names and, by making use of existing images of the victims.

Organized crime. A continuing criminal enterprise that rationally works to profit from illicit activities that are often in great public demand.

Ownership and possession analysis. Type of analysis that is used to determine the person who created, accessed, and/or modified files on a computer system.

Roasting. Individuals willingly posting images and/or videos of themselves on online and inviting others to post insults about them.

Routine activity theory. A theory that holds that crime occurs when two elements are present - a *motivated offender* and a *suitable target*, and one element is absent - a *capable guardian*.

Paedophile. A person sexually interested in children.

Passive digital footprint. Data that is obtained and unintentionally left behind by the users of the Internet and digital technology.

Patent. "Exclusive right granted for an invention (innovation or creation), which is a product or a process that provides, in general, a new way of doing something, or offers a new technical solution to a problem" (WIPO, n.d.).

Patent trolls. These individuals neither create nor invent anything; they merely purchase patents to license them to others, and sue any person, group, or organization infringing their acquired patents.

Personal autonomy. The ability to make choices and act in ways of their own choosing free from coercion.

Pharming. The creation of a fake, duplicate website that is designed to trick users to input their login credentials.

Phishing. The sending of an email to targets with a website link for users to click on, which might either download malware onto the users' digital devices or sends users to a malicious website that is designed to steal users' credentials.

Physical extraction. The search for and acquisition of evidence from the location within a digital device where the evidence resides.

Privacy. The right to be left alone and be free from observation; the capacity to keep one's thoughts, beliefs, identity, and behaviour secret; and the right to choose and control when, what, why, where, how, and to whom information about oneself is revealed and to what extent information is revealed.

Privacy by design. Privacy measures embedded in the design of systems and technologies. Also known as *data protection by design.*

Preventive law. Legal rules that focus on regulation of risk and seek to prevent crime or at the very least mitigate the damage that could be caused in the event of a crime.

Procedural law. Legal rules that cover the processes and procedures to be followed to apply substantive law, the rules to enable the enforcement of substantive law, and the rules and standards in criminal justice proceedings.

Proxy server. An intermediary server that is used to connect a client with a server that the client is requesting resources from.

Pseudonymization. The process whereby identifying data in a record is replaced by artificial identifiers.

Ransomware. Malware designed to take users' system, files, and/or data hostage and relinquish control back to the user only after ransom is paid.

Recovery. The identification, creation, and ultimate implementation of measures for resilience and the restoration of systems, networks, services, and data that were unavailable, harmed, damaged, and/or compromised during the incident.

Relational analysis. The determination of the individuals involved and what they did, and the association and relationships between these individuals.

Resilience. The ability to withstand disruptions, adapt to changing conditions, and recover from incidents of ICT and protect the confidentiality, integrity, and availability of systems, networks, services, and data.

Responsible vulnerability disclosure. The practice of not disclosing the vulnerability until a fix is provided by the responsible organization.

Risk. The impact of a threat and its probability of occurring.

Risk assessment. The evaluation of the probability of a threat, its impact, and the exposure of an asset to this threat.

Risk treatment. Responses to risks.

Script. A computer programme.

Service provider. Provides services to a computer system or a system of another digital device.

Sexting. Self-generated sexually explicit material.

Sextortion. A form of cyberharassment whereby the victim is threatened with the release of sexually explicit content if the demands of the perpetrator are not met.

Situational crime prevention. Measures used to prevent and reduce crime.

Smishing. Phishing via text messaging. Also known as *SMS phishing*.

SMS phishing. Phishing via text messaging. Also known as *smishing.*

Social engineering fraud. Tricking the victim into revealing or otherwise providing personal information and/or funds to the perpetrator.

Sovereignty. A country's right to exercise authority over its own territory.

Social dilemma. When individuals' decisions are based on self-interest rather than the interest of the group or collective, even when the utility of engaging in the collective interest is higher than the utility of engaging in self-interest.

Solipsistic introjection. The fictional image of others created by users' perceptions of others and their traits absent contextual data, including the relationships they have with them based on imagined rather than real information.

Social engineering. A tactic whereby a perpetrator tricks the target into divulging information or performing another action.

Spam. Sending of unsolicited emails.

Spearphishing. The sending of emails with infected attachments or links that are designed to dupe the receiver into clicking on the attachments or links.

Specific deterrence. Punishing individuals who commit crime to cease further illicit activity if the punishment received outweighs the benefits of committing the crime.

Spyware. Malware designed to surreptitiously monitor infected systems, and collect and relay information back to creator and/or user of the spyware.

Stalkerware. A form of spyware that can run on a victim's computer, smartphone or other Internet-enabled digital device and collect and relay all the user's actions on these devices, from emails and text messages sent and received, to photographs taken and keystrokes.

Standard operating procedures. Documents that include the policies and sequential acts that should be followed to investigate cybercrime and handle digital evidence on information and communication technology.

Steganography. The stealthy concealment of data by both hiding content and making it invisible.

Substantive law. Legal rules that govern behaviour and responsibilities of those over whom the state has jurisdiction.

Surface Web. Indexed websites that are accessible and available to the public and can be searched using traditional search engines. Also known as *Clearnet* or *Visible Web.*

Swappers. Semiautomated cryptocurrency exchanges.

Temporal analysis. The determination of the time events occurred and the sequence of these events.

Territorial sovereignty. The state's complete and exclusive exercise of authority and power over its geographic territory.

Threat. A circumstance that could cause harm.

Time-frame analysis. Type of analysis that seeks to create a timeline or time sequence of actions using time stamps that led to an event or to determine the time and date a user performed some action.

Traceback. The process of tracing illicit acts back to the source of the cybercrime. Also known as *back-tracing.*

Trade secrets. Valuable information about business processes and practices that are secret and protect the business' competitive advantage.

Trade secret theft. The theft of a trade secret offline and/or online to gain an unfair competitive advantage.

Trademark counterfeiting. Intentional unauthorized use of a trademark to label good or service that does not originate from the trademark owner.

Trademarks. Identifiers that distinguish the source of a good or service.

Traffic data. Data transmitted over a computer network (or network).

Trojan horse. Malware designed to look like legitimate software in order to trick the user into downloading the programme, which infects the users' system to spy, steal and/or cause harm.

Unallocated space. Space that is available for use because content was deleted, or space never used.

Usability. Ease with which digital devices can be used.

Visible Web. Indexed websites that are accessible and available to the public and can be searched using traditional search engines. Also known as *Clearnet* or *Surface Web*.

Vulnerability. Exposure to harm.

Virus. Malware that requires user activity to spread.

Vishing. Phishing via telecommunications.

Watering hole attack. Placing malware on the most frequented websites of targets to ultimately infect their systems and gain unauthorized access to them.

Web crawlers. Applications designed to traverse the World Wide Web to achieve specific objectives.

Whaling. Pretending to be higher level executives in a company, lawyers, accountants, and others in positions of authority and trust, in order to trick employees into sending them funds.

Worm. Stand-alone malicious software that spreads without the need for user activity.

Write blocker. Designed to prevent the alteration of data during the copying process.

Zero day. Previously unknown vulnerability that is exploited once identified.

UNODC
United Nations Office on Drugs and Crime

Vienna International Centre, P.O. Box 500, 1400 Vienna, Austria
Tel.: (+43-1) 26060-0, Fax: (+43-1) 26060-3389, www.unodc.org