Strategic partnership project within ERASMUS+
Program AGREEMENT NO. - 2018-1-RO01-KA202-049449

COURSE SYLLABUS

Strategic Communication to Counter Security Threats in the Disinformation Era

Version 1. 31/05/2020

Rubén Arcos, Irena Chiru, Mihaela Teodor, Cristina Ivan, Ileana-Cinziana Surdu, Georgios Chasapis, Vagia Poutouroudi, Andriani Retzepi, Konstantinos Tigkas, Giorgos Triantafyllou, Manuel Gértrudix

"Mihai Viteazul" National Intelligence Academy (MVNIA) – Romania, Ciberimaginario Research Group of the University Rey Juan Carlos– Spain, Kentro Meleton Asfaleias (KEMEA), Center For Security Studies – Greece and Ministry of Internal Affairs, Directorate for Information and Public Relations (MAI-DIRP) – Romania.

https://crescentproject.eu

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

DOI: 10.5281/zenodo.3870725

Table of Contents

DOI: 10.5281/zenodo.3870725

1. Course Information

1.1. Title

Strategic Communication to Counter Security Threats in the Disinformation Era

1.2. Course Description

The culture of communications is changing at a rapid pace, driven by the power of internet and social networks. The digital communication environment, with its remarkable advantages and opportunities, also provides opportunities to different actors for conducting malicious influencing activities, divide societies, erode the democratic values and sow distrust in our institutions. Users are encouraged to create personal echo-chambers at the expense of information pluralism and to move away from reliable and credible news reporting and sound journalist analyses.

This interdisciplinary course framed under the CRESCEnt project (Mind the Gap in media coverage and strategic communication in case of security threats), co-funded by the Erasmus+ Programme of the European Union, addresses the challenge of building awareness and developing resilience to disinformation, fake news, and hostile information influencing campaigns.

The MOOC aims to increase the key knowledge and competences of institutional spokespersons and journalists (including young professionals in journalism and related disciplines/areas) in the field of security and defense, and in relation to strategic communication and news reporting on security threats.

The course is developed in collaboration between: "Mihai Viteazul" National Intelligence Academy (MVNIA) – Romania, Ciberimaginario Research Group of the University Rey Juan Carlos– Spain, *Kentro Meleton Asfaleias* (KEMEA), Center For Security Studies – Greece and Ministry of Internal Affairs, Directorate for Information and Public Relations (MAI-DIRP) – Romania.

DOI: 10.5281/zenodo.3870725

1.3. What you will learn

- Understand the 21st security threat landscape and the role of the cyber/information as security dimension.
- Analyze the key concepts related with communication processes: disinformation, misinformation, propaganda, covert influencing, digital active measures, strategic communication, and hybrid threats.
- Acquire competencies and analytic tools in order to evaluate information sources and contents, and critically address the consumption of information in traditional media and social media channels.
- Plan strategic communication campaigns with a particular focus in tackling security threats
- Understand the importance of sound and responsible journalist practices, and of bridging the gap between media professionals and institutional strategic communicators in case of security threats, for addressing the challenge of fakes news and deliberate disinformation activities.

1.4. Requirements

A previous knowledge of communication studies (disinformation, propaganda, media literacy, and fake news) just as in the field of security/ law enforcement is recommended to take advantage of the course.
However, it can be followed by anyone with an interest in the subject of strategic communication.
The course is specifically designed for institutional spokespersons, students in communication and journalism and young journalists and opinion leaders that take part in accredited media communication flows during major security events.

Onsite

The course is aimed at institutional spokespersons and journalists who communicate on issues related to security and law enforcement, as support in their professional activity.

Online

The course is especially aimed at institutional spokespersons and journalists who communicate on issues related to security and law enforcement, as support in their professional activity. In any case, it is of interest to active journalists and spokespersons, journalism students, and any other professional interested in improving their knowledge about how to identify fake news, disinformation and misinformation through different sources of information generating resilience to them.

1.5. Course materials

The course uses different resources in both its onsite and online versions: interactive videos, infographics, videoclasses and self-evaluations. In each subsection the contents are presented by blocks with reflective activity proposals.

The student will be able to watch the videos, interact with the dynamic infographics and participate in the forum to share your knowledge, consult the facilitator and exchange ideas with the rest of the students on the course.
At the end of the section, the student will have to complete the evaluation of the section to measure your learning.
In addition, in the different sub-sections there are a complete list of bibliographical references and other resources that will help the student to go deeper into the contents of this week.

2. Student Learning Outcomes

2.1. Skills

Students will achieve the following professional skills:

- Identify fake news, disinformation and misinformation through different sources of information generating resilience to them.
- Deal with the production of information and reporting in its professional activity under ethical and deontological criteria.
- Review and check the sources of information before preparing a report using double fact-checking techniques.
- Report security threats truthfully.

2.2. Objectives

The course has the following objectives:

- Enhance key-competences and skills to:
    - Become resilient to fake news.
    - Build an ethics of reporting and provide and abide by ethical grounds in handling sources.
    - Perform double fact-checking.
    - Report security threats truthfully for the preservation of democracy and the rule of law.
- Raise the level of awareness in the field of fake news, disinformation, hybrid threat, social polarization, radicalization, extremist violence, and terrorism
- Improve specific skills to identify and understand their implications over the society.
- Support the participants to deal in their professional activity with responsibilities in managing strategic communication.

2.3. How you will achieve these goals

You will meet the objectives listed above through a combination of the following activities in this course: Attend, Complete, Participate, Test…

3. Topic Outline

3.1. Workload of student

On-site		Online	
Duration:	5 days	Duration:	5 weeks
Hours:	25	Estimated effort:	25h

3.2. Structure of Syllabus

Section 1. Security, asymmetric threats, and communication

- Subsection 1.1. Characterization of the 21st Century security threat landscape. Definitions: national security threats, state conventional and non-state unconventional methods, Hybrid threats, disinformation
- Subsection 1.2. What are the main security threats affecting European liberal democracies in the digital era?
- Subsection 1.3. Cyber/Information as a security domain. Individuals and institutions as the targets of hostile state and non-state actor activities: addressing the security challenge
- Subsection 1.4. Evaluation of the Section

Objectives:

The main objective of the section is knowing and understanding essential concepts on security, asymmetric and hybrid threats, and communication.
To this end, we will work on these specific objectives:

- To determine what are the characteristics that define the 21st Century security threat landscape.
- To review some definitions like national security threats, state conventional and non-state
- unconventional methods, hybrid threats or disinformation.
- To discuss how the main security threats are affecting European liberal democracies in the digital era.
- To identify Cyber/Information as a security domain.
- To provide a summary of the main points works this week and assess of how far you reached in
- understanding the concepts and tools presented.

Contents:

- Fundamental concepts about security, asymmetric and hybrid threats, and communication. These concepts are key for making progress in the course.

DOI: 10.5281/zenodo.3870725

- Specifically, we are going to study:
  - The characterization of the 21st Century security threat landscape. Definitions: national security threats, state conventional and non-state unconventional methods, hybrid threats, and disinformation.
  - The main security threats affecting European liberal democracies in the Digital Era
  - Cyber/Information as a security domain. Individuals and institutions as the targets of hostile state and non-state actor activities: addressing the security challenge
  - The EUvsDisinfo project
  - Finally, we will make a first evaluation to know if you have understood well all the concepts worked on.

Methodology and resources

- To achieve the set objectives, in this section you will find different resources: interactive videos, infographics,
- Video-classes and self-evaluations. In each subsection the contents are presented by blocks with reflection activity proposals
- Read, watch the videos, interact with the dynamic infographics and participate in the forum (in the case of the MOOC) to share your knowledge, consult the facilitator and exchange ideas with the rest of the students on the course.
- At the end of the section, you will have to complete the evaluation of the section to measure your learning.
- In addition, in the different sub-sections we have prepared complete lists of bibliographical references and other resources that will help you to go deeper into the contents of this week.

Section 2. Strategic Communication and Public Opinion

- Subsection 2.1. Strategic communication phenomena: Strategic communication as a process; Models of communication; Propaganda, misinformation, and disinformation.
- Subsection 2.2. What is Public Opinion? Approach to concepts of public and opinion. Communication and Public Opinion. Information and opinion. Opinion and news media. Theories.
- Subsection 2.3. Strategic planning of communication, Publics/stakeholders analysis, RACE/ROPE/RPIE Process, Communication tactics
- Subsection 2.4. Evaluation of the Section

Objectives:

The main objective is knowing the fundamental concepts of Strategic Communication and Public Opinion

To achieve this, we will work on these specific objectives:

- To interpret the strategic communication phenomena from the premise that communication can be studied as a process from different models.
- To know what is Public Opinion and the links between Communication and Public Opinion.
- To differentiate some fundamental Theories about Public Opinion.
- To understand the importance of strategic planning of communication and how apply some analysis and communication tactics.
- To assess how far you reached in understanding the concepts and tools presented.

Contents:

The fundamental concepts of Strategic Communication and Public Opinion.
Specifically, we will see:

- Strategic communication phenomena: Strategic communication as a process; Models of communication; Propaganda, misinformation, and disinformation. Wardle and Derakhshan's Information disorder framework
- What is Public Opinion? Approach to the concepts of public and opinion. Communication and Public Opinion. Information and opinion. Opinion and news media. Theories. Opinion and news media
- Strategic planning of communication, Publics/stakeholders analysis, RACE/ROPE/RPIE Process
- Communication tactics.
- Lastly, we will provide a summary of the main points works this week and also an assessment of how far you reached in understanding the concepts and tools presented.

Section 3. Addressing the challenge of fake news, disinformation and covert influence in the digital era

- Subsection 3.1. Propaganda and disinformation in historical perspective
- Subsection 3.2. Ethics and journalism for countering disinformation/misinformation
- Subsection 3.3. Covert influence and the challenge of attribution. Communication-led covert actions. Plausible deniability. To what extent is attribution possible?
- Subsection 3.4. Evaluation of the Section

Objectives:
The main objective is addressing the challenge of fake news, disinformation, and covert influence in the Digital Era.
To achieve this, we will work on these specific objectives:

DOI: 10.5281/zenodo.3870725

- To know the historical evolution of propaganda and disinformation and the essential changes occurred in relation to means and methods used through the ages.
- To analyze the ethics and journalism resources for countering disinformation/misinformation.
- To identify how currently both state and non-state actors can use social media to employ time-tested propaganda techniques to reach large audiences and extremely impactful results.
- To evaluate your understanding of the concepts and contents work during this week.

Contents:

We will address the challenge of fake news, disinformation, and covert influence in the Digital Era.

- Propaganda and disinformation in historical perspective presents in an interactive timetable the historical perspective on propaganda and disinformation. We tried to present not only important moments in the evolution of the phenomenon of propaganda and disinformation, but essential changes occurred in relations to means and methods used through the ages.

- The disinformation playbook in 21st Century analyze ethics and journalism for countering disinformation/misinformation. Experts views on disinformation: failed messages, fake news and ethical aspects. When our message is failed, we may reinforce misinformation/disinformation.

- Covert influence and the challenge of attribution show how due to changes in technology and the media, currently both state and non-state actors can use social media to employ time-tested propaganda techniques to reach large audiences and extremely impactful results. But attribution in online disinformation campaigns is a complicated endeavor, because it is not entirely possible to define the source, the funding of the disinformation campaign or whether it had a domestic or international effect.

- Finally, we provide an assessment of your understanding of the concepts and contents and present a summary of the key topics covered in "Addressing the challenge of fake news, disinformation, and covert influence in the Digital Era."

Section 4. CRESCEnt Advanced Analytic and Critical Thinking Toolkit

- Subsection 4.1. Evidence, judgement, and logical reasoning
- Subsection 4.2. Information evaluation and verification 101: Source reliability, content credibility, audiovisual material checking

- Subsection 4.3. Disinformation/propaganda analysis: Identifying and exposing hostile information influencing
- Subsection 4.4. Evaluation of the Section

Objectives:

The main objective of this week is to learn learn how to correctly manage the process of logical reasoning to reach correct conclusions using the CRESCEnt Advanced Analytic and Critical Thinking Toolkit.
To this end, we will work on these specific objectives:

- To know the process of logical reasoning and the types of implications that lead to conclusions.
- To review the types of fallacies.
- To learn how check the source reliability, content credibility
- To learn how check audiovisual material.
- To identify hostile information influencing and its modus operandi.
- To know what strategies and tools we can be used for identification and exposure.

Contents:

In the section we will learn about the main aspects of the CRESCEnt Advanced Analytic and Critical! Thinking Toolkit developed through this project co-fiunded by the European Union's Erasmus+ programme.
Specifically, the following contents are worked on:

- "Evidence, judgement and logical reasoning" discusses the process of logical reasoning and the types of implications that lead to conclusions. It proposes a series of principles to be followed in order to avoid errors and identify logical fallacies and stresses the importance of evidence and judgement in argumentation. Types of informal fallacies are also reviewed, as support in the activity of strategic communication.
- Information evaluation and verification 101 examines source reliability, content credibility, and audiovisual material checking.
- "Disinformation/propaganda analysis: Identifying and exposing hostile information influencing" presents the main features of covert information operations, their modus operandi, as well as what strategies and tools we can use to identify and expose them. Special focus is being placed on propaganda, disinformation, information warfare tactics, and the emerging technologies that can help us in the timely detection and uncovering of their shady purposes.
- Finally, it is provided an assessment of your understanding of the concepts, contents, and tools presented and it presents a summary of the key topics addressed in Section 4 "CRESCEnt Advanced Analytic and Critical Thinking Toolkit".

Section 5. Role-playing Simulations/Gaming

- Subsection 5.1. Countering disinformation with professional and ethical journalism: hands-on hard news reporting and analysis journalism. Role-play as journalist and produce a news story and interpretative piece using open sources
- Subsection 5.2. Everything fake: Detecting AI-generated forgeries (GAN)
- Subsection 5.3. Strategic Communicator game challenge
- Subsection 5.4. Evaluation of the Section

Objectives:

The main objective of is to learn “hands-on” how to counter disinformation with professional and ethical journalism. To do this we will assume the role of a journalist, we will try to detect AI-generated forgeries (GAN) and we will test ourselves as strategic communicators in a crisis.

In addition, we will work on these specific objectives:

- To understand the differences between journalism genres: hard news reporting, interpretive journalism, and opinion.
- To know the golden rules of ethical journalism useful in countering disinformation.
- To take the role of a journalist and produce a news story and interpretative piece using open sources.
- To train analogic and Deepfakes detection
- To apply strategic communication strategies

Contents:

We will work on some contents that will help you to face ethically, as a journalist or as a spokeperson, the challenges of fake news and disinformation as well as situations in which you will have to apply the strategic communication.

- Journalism genres: understanding the differences between hard news reporting, interpretive journalism, and opinion
- The golden rules of ethical journalism useful in countering disinformation
- Role-play as journalist and produce a news story and interpretative piece using open sources.
- Images generated by Deepfake technology
- How to spot Deepfake images of people
- Practice the spotting of Deepfakes based on the training received
- Conspiracy theories about the coronavirus
- Role-play as a strategic communicator addressing the coronavirus pandemic
- Recommendations for strategic communications in fighting disinformation

- Tips that can help you crafting a response during crisis

4. Grading Policy - Certification

4.1 Onsite (Blended learning)

a. Grade Course Activities

The student must attend 90% of the sessions, carry out the planned activities and pass the final evaluation questionnaire.

b. Certification

Course participants will receive at the end of the on-site course:

1. Europass Mobility Certificate, which will be incorporated into the CPD of the organizations.
2. Participating diplomas. Training certificates for participants detailing the learning outcomes and key competences to recognize professional and personal development for all participants.

4.2. Online (MOOC)

a. Grade Course Activities

To obtain the completion badge is obtained automatically when you pass, at least, an average of 80% of all the obligatory activities of the course.

b. Certification

The completion of the MOOC will allow the following accreditations to be obtained:

1. Completion badge.

   At the end of a MOOC, you will receive a free digital emblem that accredits the successful completion of the MOOC's activity plan. If necessary, specific badges linked to intermediate activities of the MOOC may be awarded. This badge will be used to show the skills acquired in social networks (LinkedIn, Facebook ...) on your website or in any other digital space.

2. Accreditation of overcoming

   Participants will be able to apply for a digital certificate when they have passed all the obligatory activities of the course. The certificate will reflect that they have successfully completed the course and will include the number of hours of the course.

   The cost of the accreditation will be the one established by the URJCx platform and is carried out directly through the platform's online system, on previous request.

DOI: 10.5281/zenodo.3870725

5. Course Policies

5.1. General

Commit to Integrity

As a student in this course you are expected to maintain high degrees of professionalism, commitment to active learning and participation in this class and also integrity in your behavior.

Academic Dishonesty Policy

Academic dishonesty includes such things as cheating, inventing false information or citations, plagiarism and helping someone else commit an act of academic dishonesty. It usually involves an attempt by a student to show possession of a level of knowledge or skill that he/she does not possess. Any form of academic dishonesty, including cheating and plagiarism will be cause of exclusion.

5.2. Specific rules for the online course (MOOC)

Who can do the MOOC?

The MOOC is studied through the URJCx platform, so it is part of the open training offer of the Rey Juan Carlos University. Thus, it will be available for anyone to access and participate for free.

To join a course, it is enough to have a computer connected to the Internet, an updated browser and the desire to improve through community learning.

How can I register?

You will have to complete the registration form to register in URJCx.

When does the MOOC start and end?

Information on the start and end dates of each edition of the MOOC is available on the MOOC description page. Also, if you've already signed up for a MOOC, you'll be able to see the start date in your control panel.

Due to time differences, the start time of a course may vary within the specified date depending on the country or time zone from which it is accessed. Keep this in mind for both the start and end of the course.

If you log in during the start date and the course is not yet available, try logging in again throughout the day.

How do I communicate and interact with course facilitators, curators or participants?

All the communications of the course are done through the channels (spaces and networks) of the MOOC itself, where all the activity is concentrated among the course participants. This type of course does NOT include e-mail communication with the teaching staff.