Exploring, Understanding and Doing Interdisciplinary Education: A Three-Step Approach to guide Lecturers and Students through Interdisciplinary Analysis of Complex Security Challenges

Prof.dr. Bibi van den Berg*, dr. Ruth Prins

Leiden University, Faculty of Governance and Global Affairs the Hague, The Netherlands

*Corresponding Author: **Prof.dr. Bibi van den Berg,** *Leiden University, Faculty of Governance and Global Affairs the Hague, The Netherlands. Email: b.van.den.berg@fgga.leidenuniv.nl*

Abstract: *Security challenges are highly complex; they are wicked, interdependent and have global reach and impact. Both grasping and solving these challenges requires input from various academic perspectives. As a result, the education of future security scholars and professionals requires an interdisciplinary approach. We present a newly developed teaching approach – tailor-made for a new bachelor's programme Security Studies at Leiden University – for interdisciplinary teaching and learning named 'Explore, Understand, and Do' (EUD) that can be used for interdisciplinary assessment of a wider range of complex global challenges.*

In this article, we explain the EUD approach and its theoretical basis, and how it can be implemented on both course and case level. We share our first experiences of how the EUD approach proves to be a guide for teachers when designing a courseand for students during their interdisciplinary analysis of real-life security cases. Finally, we reflect on the conditions that will enhance the effectiveness of EUD as an approach for teachers and students. A crucial factor in order for students and lecturers to be successful in their endeavours proved to be a basic knowledge about academic inquiry and scientific disciplines before applying EUD on both course and case level.

Keywords: *Interdisciplinary, Interdisciplinarity, Education, Security, Teaching approach*

1. INTRODUCTION

Contemporary public problems, such as climate change, public health, migration and security, are incredibly complex and require multifaceted strategies. They call for professionals being able to deal with complexity and bridge perspectives in order to devise proper solutions. As a response, a substantive number of interdisciplinary educational programmes have been created in higher education over the past decades to teach students about this type of challenges (Spelt, Biemans, Tobi, Luning & Mulder, 2009). The appeal to interdisciplinary education stems from the assumption that it will equip professionals to address today's quickly changing and multifaceted world. This shared ambition, in turn, leads to a demand for educational formats that deliver the promise of interdisciplinary education. In other words, it creates a need to move forward in designing and empirically testing teaching methods for interdisciplinary education.

This paper presents a new approach to interdisciplinary teaching and learning for university education on bachelor level by demonstrating the case of Security Studies at Leiden University, the Netherlands[1]. This new academic bachelor's programme in Security Studies aims to train students in interdisciplinary assessment of contemporary security challenges, such as terrorism or cyber security, and natural hazards, such as earthquakes or hurricanes. These challenges have complex causes and consequences; they cut across state and institutional boundaries and oftentimes there is no straightforward solution available. Consequently, one needs to borrow insights from a wide variety of academic disciplines to arrive at a deeper understanding of complex security challenges. In order to facilitate interdisciplinary teaching and learning about security challenges, we developed a new teaching approach titled 'Explore, Understand and Do', or 'EUD'.

---

[1]The first cohort of this program started in September 2017.

This paper introduces this new teaching approach and aims to help lecturers design interdisciplinary courses as well as equip students with practical tools to carry out interdisciplinary analysis. We begin by arguing why modern-day security challenges could be assessed best in an interdisciplinary way. This is followed by explaining how we define interdisciplinarity, after which we introduce 'Explore, Understand and Do' as our three-step approach for interdisciplinary teaching and learning. We take real-life examples and best practices from the security domain to demonstrate and explain our approach. After that, we explain how we implemented this approach on course and case level in the Security Studies bachelor's programme. We will close off with some reflections on how to use and further develop this teaching philosophy to carry out interdisciplinary analysis of other complex challenges present in today's globalised world.

2. THE NEED FOR AN INTERDISCIPLINARY APPROACH TO MODERN-DAY SECURITY CHALLENGES

Security challenges rank among the most pressing issues of our time. One cannot turn on the news, scroll through one's timeline or enter a public space without being confronted with all sorts of security challenges, such as terrorism, cyber security, industrial disasters, international conflicts and global warming. Security issues dominate the news and worry citizens. They cause governments and businesses to spend large sums of money on all sorts of security measures. In other words, security is a pervasive societal theme.

What modern-day security challenges have in common is the fact that they are by no means easy to understand or solve. Scholars qualify security challenges as highly 'wicked' and interconnected. Security challenges are *wicked problems* because they often have multiple, interlinked and changing causes because stakeholders disagree about the most appropriate solution and because addressing them means spending scarce resources and impacting the lives of human beings (Rittel & Webber, 1973).The current debate about terrorism, for example, centres around questions suchas : are acts of terrorism driven by religious ideas, social exclusion, political aspirations and/or by psychological mechanisms such as identity searches and disconnection? Experts are puzzled about the question whether it is even possible to prevent terrorism by focussing on one or more of these factors or if we should rather spend our scare resources on sanctioning and punishment. In the mean time, measures covering the entire spectrum of impacting basic human rights such as privacy and freedom of movement are already taken to combat terrorism. This includes measures such as screening individuals suspected of planning attacks and laws expanding the activities of police and army personnel, and many more. The multiple causes, uncertainty about proper strategies in light of scarce recourses and the impact on citizens makes modern-day terrorism a wicked problem.

Security challenges are also *interconnected*, meaning that they may have global reach or global impact (Western, 2016).This implies that causes and impact of a particular security challenge may be strongly connected, even if they are spread across the globe. A violent conflict in the Middle East (cause) may trigger a large stream of migrants (impact) challenging local societies and city governments throughout Europe to deal with all sorts of practical, moral and societal challenges that come with the influx of people from another continent and culture (impact). This makes security challenges multi-layered and cross both state and institutional boundaries. Therefore, they affect and connect various parts of the world, as well a wide range of actors, from local citizens to international governments and businesses and everything in between.

Taken together, the wickedness and interconnectedness of modern-day security issues calls for an *interdisciplinary approach*. Only when particular insights and methods present in various academic disciplines are selected and merged, one hopes to gain a better understanding of causes, impact and solutions to modern day security challenges. A simple example can further clarify our claim that the characteristics contemporary security challenges creates a need for interdisciplinary analysis. When aiming to understand and address cyber-crime, one needs to borrow from a myriad of academic disciplines. Psychology and Sociology offer tools to understand individual and societal factors facilitating cyber-crime. Computer Science provides tools for businesses and governments to conduct risk analysis. Public Administration and Law help to reflect on the possibilities and limitations to regulate cyber security threats. In other words, particular insights and methods present in various

academic disciplines need to be selected and merged in order to arrive at a deeper understanding of complex societal challenges.

3. SECURITY STUDIES: AN INTERDISCIPLINARY BACHELOR'S PROGRAMME

Academic inquiry of security challenges is the central activity in the bachelor's programme Security studies. We broadly define *academic inquiry* as the process of assessing real life phenomena through the lenses of academic disciplines providing theories, concepts and methods to generate insights and build knowledge. The number of disciplines and the extent to which they are integrated during the process of academic inquiry determines what kind of analysis one undertakes: mono-, multi or interdisciplinary (Klein, 2006; of Davies & Devlin, 2007; Spelt et al., 2009). As explained in the previous section the complexity security challenges creates a need for interdisciplinary analysis.

The concept of *interdisciplinarity*, though, has been defined in many ways (e.g. Klein, 2006; Davies & Devlin, 2007; Spelt et al, 2009).For the bachelor's programme Security Studies, we adopted the following definition: 'the capacity to integrate knowledge of two or more disciplines to produce a cognitive advancement in ways that would have been impossible or unlikely through single disciplinary means' (Spelt et al., 2009:1). This separates our approach from *monodisciplinary* analysis, consisting of adopting a single discipline and applying that to study a particular part of the natural, social or cultural world. Monodisciplinarity is the 'traditional' way of doing science; disciplines do not borrow from one another, rather they act as silos each working on their own problem. Interdisciplinary analysis is more closely related yet fundamentally different from *multidisciplinary* approaches (Klein, 2006; Davies & Devlin, 2007). While researchers and students conducting multidisciplinary analysis usually do combine tools from various disciplines, they use them alongside each other. As such, interdisciplinary analysis goes one step further by moving away from using disciplines in parallel to each other to merge and integrate ideas, methods, findings and approaches from various disciplines into new knowledge and ideas.

Embracing interdisciplinarity thus means that we train our students in *selecting AND integrating* tools from various disciplines to further their knowledge and understanding of complex security challenges. To enable such an analysis, we selected a set of ten academic disciplines relevant for studying contemporary security challenges central to the curriculum of the Bachelor Security Studies, as shown in figure 1.
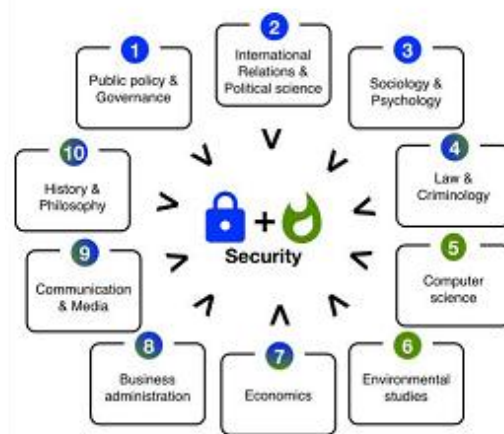

Figure1. *Academic disciplines in the Bachelor Security Studies*

Together, these ten disciplines offer a set of tools to face today's complex and multifaceted security challenges. They cover a wide range of scientific domains, from the Natural Sciences (Computer Science) and Social Sciences (Sociology, Public Administration) to the Humanities (Philosophy). Also, they provide both analytical descriptions (History, Psychology), normative prescriptions (Political Science, International Relations) and more domain specific theories, concepts and methods (Economics, Environmental Studies, Criminology). These ten disciplines are central to the processes of academic inquiry undertaken by both lectures and students in our programme.

Integration of this multiplicity of disciplines is central to interdisciplinary analysis, yet there is not one proven recipe, or pedagogy, that supports the process for either teachers or students (Klein, 2006: 15). Klein did find however, that a connection exists between interdisciplinary education and innovative teaching methods that rely on an active role of students, both in the discovery of relevant knowledge and in making sense of the implications of that knowledge. This active role in the learning process requires students to develop and apply 'soft skills', such as critical thinking, communication, teamwork, and other related competences (Vogler, Thompson, Davis, Mayfield, Finley &Yasseri, 2017). Our teaching approach Explore, Understand and Do helps students design and carry out their academic endeavours in an interdisciplinary manner by actively engaging in a three-step process of academic inquiry in which these skills are required every step of the way.

4. EXPLORE, UNDERSTAND AND DO: A THREE-STEP APPROACH FOR INTERDISCIPLINARY ANALYSIS

Following our understanding of interdisciplinarity, one has to know and do a couple of things in order to arrive at a genuine interdisciplinary assessment of a security case. The trick is to select a set of *relevant disciplines* needed to answer a particular research question about the case. The next challenge is to choose the relevant *tools* a discipline has to offer in light of the research question and case to be studied. By tools we mean *theories, concepts and research methods* belonging to a particular discipline helping to understand and assess particular elements of a real-life phenomenon. After that, these tools should be applied to the case and the insights and knowledge one generates should be integrated in order to arrive at a deeper, interdisciplinary understanding of the case. All of this can only be done when one has a certain level of *background information* about the security case at hand as well as some knowledge of the various disciplines and tools available. Only then is it possible to make an informed choice of disciplines to be adopted and merged in an interdisciplinary analysis.

We developed a teaching approach to help lecturers design interdisciplinary courses and equip students with practical tools to carry out interdisciplinary analysis. Our approach relies heavily on *case-based learning*. Central to our interdisciplinary teaching activities are real-life security challenges we assess by means of three steps Explore, Understand and Do, as shown in figure 2. This means that both lecturers and students choose a real-life security case and assess it by following the basic steps of interdisciplinary analysis.
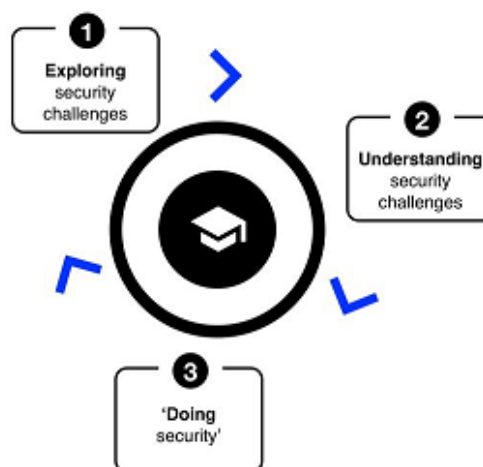

Figure2. *The three steps Explore, Understand, Do*

The successive steps of Explore, Understand and Do facilitate interdisciplinary analysis of complex cases by first exploring crucial events, actors and context (Explore), followed by making an informed selection of theoretical insights and research methods from a wide variety of academic disciplines and apply them to an empirical case (Understand). This eventually leads to an integrated and interdisciplinary analysis of causes, impact and solutions (Do). Once these three steps have been undertaken for the first time, one can go backwards and forwards to refine one's analysis in an

iterative manner. While analysing a particular element of the case during the understanding phase, one may, for example, discover a need for additional or new empirical information in order to fully apply a theoretical lens, thus one may go need to go back to the exploring phase.

4.1. Explore

During the exploration phase, students collect facts and figures of real-life events, actors and their actions which played a crucial role at some point in time in the particular case study. This is done by reconstructing a timeline of empirical facts that shed light on the (causal) chain of events. Besides collecting factual information on the case, students are invited to explore the historical, cultural and geographical context in which the security challenge happened as well. Together, this can be plotted into a case description. By exploring the case, students gain basic knowledge about the security case at hand, enabling them to conduct further research and formulate a research question. Most importantly, this research question serves as point of departure to select relevant disciplines during the following phase.

4.2. Understand

During the understanding phase, students move from collecting information to identifying relevant disciplinary lenses and applying them to the case. Students weigh and select their disciplinary lenses from the ten disciplines central to the programme and previously made available to them. Steered by their research question and basic knowledge of the case, students select several disciplines that offer relevant tools (methods, concepts or theories) for their research project. Students now engage in academic inquiry by applying their disciplinary lenses to the case that offer students insights into causes, effects and impact of the security case at hand. Understanding a security case means unravelling complex security challenges by seeing them through a set of disciplinary lenses. By combining tools that different disciplines have to offer, students acquire the skill to break down the complexities of the case into a set of distinct, yet interrelated, problems. In the process, they may develop a rich, detailed understanding of the case at hand.

4.3. Do

During the third phase students 'do security'. During this step, students undertake two activities. First of all, students complete their interdisciplinary analysis by integrating the research findings generated during the Explore and Understand phases. Students learn to see the interlinkages between concepts, theories and ideas from various disciplines, empirical data and how this provides a deeper understanding of security challenges. Seeing these interlinkages will enable them to answer their research question. Second, students assess and design strategies and solutions to address security challenges. They are invited to translate their research findings into lessons learned in terms of practices and strategies adopted by actors involved in the case. They use their freshly gained interdisciplinary insights to formulate recommendations for security strategies. What can we learn from the interdisciplinary analysis of this particular case about addressing comparable modern-day security challenges? In other words, how can we *do security* better in the future?

4.4. First Applications of EUD

With the start of the new bachelor's programme Security Studies, our new teaching approach 'Explore, Understand and Do' was implemented for the first time, both on course and case level. However, in order to actually enable students to engage in interdisciplinary analysis of security challenges by applying EUD, we first familiarised them with the basics of scientific inquiry and our set of ten academic disciplines. The programme started with an introduction course providing answers to fundamental questions such as what is science? What is an academic discipline? Which types of disciplines are out there and how do they perceive and assess the outside world? Learning about disciplines is essential to successful interdisciplinary education. After all, students must be taught about learning (to speak) a disciplinary language first (Davies & Devlin 2007). The introduction course was followed by a core course during which an interdisciplinary team of lecturers demonstrated how to conduct an interdisciplinary study of a real-life case. Here we used our teaching philosophy Explore Understand and Do on the course level. Then we asked our students to carry out interdisciplinary analyses of security challenges themselves by using EUD on the case level.

With this set-up, we deliberately timed the application of EUD on the course level by lecturers before students have to apply it themselves on the case level. This allowed us to first demonstrate how to carry out an interdisciplinary analysis of a security case in class on course level, after which students were invited to carry out an interdisciplinary analysis themselves by trying to answer a specific research question about a particular case, thus on case level. This gradually increases the level of intensity: from understanding interdisciplinarity (introduction course), to demonstration of interdisciplinary analysis (course level) to doing interdisciplinary analysis independently (case level).

4.5. EUD on Course Level: Core Course Fukushima

The bachelor's programme offers core courses designed around a specific security topic. The overall objective of these eight-week courses is to familiarise students with typical modern-day security challenges and to demonstrate how to assess them academically in an interdisciplinary way. To safeguard the interdisciplinary character of the course, its structure relies heavily on the three steps of our teaching approach. One of these courses is centred around the Fukushima disaster in Japan in 2011 and is structured along the lines of Explore, Understand and Do.

4.5.1. Exploring the Fukushima Disaster

During the first two weeks of the course, lecturers explore the case. They explain how an unfortunate chain of events, which began with an earthquake that caused a tsunami that hit a nuclear plant located near the Japanese coast in a town called Fukushima. They explain how this chain of events impacted people and the natural environment. They explore how relevant actors, such as the plant owners, the national government and the media acted before, during and after the incident. Moreover, they lecture on Japanese popular and corporate culture to help contextualise risk perception and crisis response in this case. Together, this provides an overall, empirical introduction to the case in terms of events, actors and context.

4.5.2. Understanding the Fukushima Disaster

During week 3, 4, 5 and 6 of the course, lecturers move to the understanding phase by introducing students to a set of relevant disciplinary lenses and demonstrating which sub elements of the case they help to unravel. These include Computer Science, offering (mathematical) models to assess the risks of nuclear disaster caused by extreme weather events; Engineering Science, providing criteria to assess to what extent the plant was designed to withstand a tsunami; Media and Communication Science, offering concepts to evaluate the communication strategies deployed by the prime minister of Japan and plant owner Tepco to warn and instruct citizens; and Environmental Science, prescribing methods to assess long term impact of the nuclear disaster on the natural environment. Together, these disciplines and tools provide a deeper understanding of several fundamental parts of the Fukushima disaster.

4.5.3. Doing Security in light of the Fukushima Disaster

After applying these disciplinary tools to the case of Fukushima, lecturers merge the findings on sub-elements of the case assessed during the understanding phase in week 7 and 8. These sub-elements include risk calculation and preparation, preventative measures in buildings, effectiveness of communication strategies and long-term harm to humans and animals in the Fukushima area. This results in a deeper understanding of the cascading causes, various interrelated impacts and the way in which actors intervened. Special attention is paid to the interlinkages between findings on causes, interventions and outcomes in order to unravel the complexity of the case. Moreover, the findings of this interdisciplinary analysis are translated into further recommendations for 'doing security'. One could think of strategies for dealing with small risks with high impact, best practices in crisis communication and ways to increase safety at nuclear plants.

4.6. EUD on Case Level: Assessing Hurricane Harvey

The following impression of an interdisciplinary assessment of case of Hurricane Harvey (USA, 2017) provides an example of application of EUD on a case level. For this assignment, students are invited to conduct and interdisciplinary assessment of Hurricane Harvey and are instructed to focus on the role of government organisations vis-a-vis citizens in the handling of this security case.

4.6.1. Exploring Security in relation to the Hurricane Harvey Case

During the exploration phase, students collect facts and figures on the case. They will find out that on August 25, 2017, Hurricane Harvey, a Category 4 hurricane, made landfall on the eastern coast of Texas, USA. Accompanied by a storm surge and 33 trillion gallons of rain, Hurricane Harvey caused floods in a large part of eastern Texas (Shultz & Galea, 2017; Sebastian et al., 2017). Almost 80 people died directly or indirectly due to the hurricane. More than 120.000 buildings sustained water damage. The recovery costs are still undetermined, but recent estimates are up to US$ 180 billion (Sebastian et al., 2017). Crucial actors in this case are citizens, crisis response professionals, and US government institutions.

Informed by their exploration, students formulate a research question. They could, for example, choose to analyse how US government institutions handled and sought to minimise risks for citizens who live in the area affected by Hurricane Harvey by formulating the following research question: How did US government institutions handle risks for citizens, before, during and after Hurricane Harvey?

4.6.2. Understanding Security in relation to the Hurricane Harvey Case

Moving towards interdisciplinary assessment, students select three disciplinary lenses to help understand how US government institutions operated before, during and after Hurricane Harvey. Three potential disciplinary lenses shedding light on the role of government organisations vis-a-vis citizens during Harvey are 1) Environmental Science, 2) Organisational/Management Science, and 3) Public Administration.

First, by making use of the tool of 'forecasting', from the discipline Environmental Science, students can indicate the magnitude and likeliness of extreme weather events. Applying this tool to empirical data on the Hurricane Harvey case shows that, and why, the coast of Texas is prone to floods and hurricanes. In light of the research question, students learn that hurricanes cannot be prevented, but the financial or physical impact of such an extreme weather event can be reduced for citizens by government institutions. In case of Hurricane Harvey, FEMA (the US Federal Emergency Management Agency) recognised these forecasts and urged citizens who live in flood risk areas to take out flood insurance or renew their insurance contracts. FEMA extended the period after Hurricane Harvey so survivors had the opportunity to arrange the insurance for longer than usual (FEMA, n.d.; FEMA, September 4, 2017).

Second, by applying the concept of *interorganisational decision-making* borrowed from the discipline Organisational/Management Science, students are able to analyse the US governmental institutions' strategy when cooperating with societal organisations and volunteers during evacuation of survivors. Various models for interorganisational collaboration could be adopted in practice. Analysis shows that in this particular case professional, governmental emergency responders made use of citizen potential by including the so-called 'Cajun Navy', a voluntary citizen initiative, in their evacuation activities. This is a rare strategy for US crisis management. During previous disaster management efforts, for instance during Hurricane Katrina (2005), US government action mostly resembled the traditional and hierarchical model of 'command and control', causing crisis managers to exclude non-government organisations from the response efforts (Comfort, 2017; Aldrich, 2010).

Finally, after Hurricane Harvey dissipated, the immediate risk for citizens diminished. However, long-term risks, such as mental and physical health problems and economic loss still exist for the community (Aldrich, 2010; Shultz & Galea, 2017; Sebastian et al., 2017). The discipline Public Administration offers the concept of Resilience, allowing students to indicate the extent to which US government organisations boosted societal capacity to anticipate and recover from long-term risks; after Hurricane Harvey. Application of this tool demonstrates that US government institutions activities did not primarily focus on resilience nor long-term risks. US government institutions mostly undertook traditional disaster recovery activities, such as repairing damage to infrastructure, supplying monetary resources for survivors, providing information about other resources citizens may qualify for, and providing temporary housing (Aldrich, 2010; Sebastian et al. 2017). Although academic research has found that social capital of a community is an influential factor for efficient

recovery after a crisis and it is possible for governments to influence social capital positively through implementation of resilience-oriented policies (Aldrich, 2010), there are no reports of efforts of US government institutions during Hurricane Harvey that fall under this category.

4.6.3. Doing security in light of the Hurricane Harvey case

In the doing phase students will integrate the various insights offered by different disciplinary tools and answer the research question: How did US government institutions handle risks for citizens, before, during and after Hurricane Harvey?

From the previous case analysis, it is possible to conclude that US government institutions act and provide resources for citizens to reduce risk and impact before, during and after Hurricane Harvey. More specifically, we learned they actively participate in risk forecasting *before* the hurricane and align their actions to those forecasts (Environmental Science - Forecasting). *During* the crisis-response phase, US institutions no longer relied on traditional crisis management models structuring collaboration between government agencies (Organisation Science – Interorganisational Collaboration). While doing so, US government institutions strategically made use of citizen potential during immediate crisis response activities. However, US government institutions did not actively make use of societal capital (Public Administration - Resilience) to diminish *long-term risks* for survivors of Hurricane Harvey.

In terms of 'doing security', we can draw several lessons from this interdisciplinary analysis on the role of government organisations vis-a-vis citizens in the handling comparable security cases:

- Forecasting is a useful tool to raise awareness of risks amongst state actors and citizens enabling both parties to protect themselves against future harm.

- Governmental crisis response activities can benefit from including resources societal actors have to offer.

- Investing in resilience and social capital supports efficient recovery of communities after a crisis and subsequently decreases the long-term impact and risks for citizens.

To summarise, applying EUD on the course level implies adoption of our three steps of interdisciplinary analysis into the overall course structure in order to demonstrate interdisciplinary case study in plenary sessions. EUD on the case level, on the other hand, is about students carrying out interdisciplinary assessment themselves and offers practical steps to design and plan their activities.

4.7. Reflection: First Experiences and what is Next?

The complexity of modern-day security challenges calls for an interdisciplinary approach. The bachelor programme Security Studies at Leiden University embraces a case-based learning strategy in order to make interdisciplinary analysis happen. To structure and facilitate the process of interdisciplinary teaching and learning, a three-step teaching approach was developed and implemented for the first time in 2017. This approach, called 'Explore, Understand and Do', helps both lectures and students to break down the process of interdisciplinary analysis into three basic steps: 1) explore the real-world dynamics of a security case (explore), 2) borrow and merge relevant theories, concepts and methods from selected disciplines and apply them to empirical data (understand), and 3) merge research findings into an interdisciplinary understanding of the case based on which strategic recommendations can be made (do).This teaching approach could be applied on both course and case level.

The first experiences with implementing Explore, Understand and Do as a teaching approach for interdisciplinary teaching and learning are positive. The three-step approach serves as a tool to familiarise first-year students with interdisciplinarity, both on a conceptual (what is it?) and practical level (how to do it?). This practical approach helps both lectures and students locate themselves in the academic world (what academic discipline are out there? and what are they for?), the process of academic inquiry (how to assess real world cases academically?) and the key steps of interdisciplinary analysis (how to select, apply and merge disciplinary insights?).

Our approach to guide lecturers and students through interdisciplinary analysis is certainly not restricted to security challenges alone. The three steps of interdisciplinary analysis could easily structure analysis of any complex societal challenge as long as there is a real-world case to be studied for which empirical data is available. When adopting this strategy, our experiences taught us that one needs to take into account two crucial factors for further fine-tuning and wider usage of Explore Understand and Do (EUD) facilitating interdisciplinary teaching and learning:

First, the application of EUD requires some pre-existing knowledge of academic inquiry and the very existence of relevant disciplines in order to make informed choices while selecting relevant disciplines and disciplinary tools (c.f. Spelt et al., 2009; Davies & Delvin, 2007).This is of the utmost importance for (first-year) students. We addressed this need by preceding EUD with an introduction course explaining the fundamentals of academic inquiry and familiarising students with a set of academic disciplines. This proved to be an effective way to get first-year students up to speed in an interdisciplinary programme. More senior students might already have basic knowledge of science and disciplines, but do need to be made aware of the fact that they need to explicitly take this as their point of departure to successfully participate in interdisciplinary exercises. One way or the other, one should always make sure students have a basic knowledge of science and disciplines, enabling them to actually engage in interdisciplinary adventures.

Second, the application of EUD on the course level works best when done by a team of lecturers who have mastered one or more disciplines central to the course. Developing and teaching interdisciplinary courses and assignments requires deep knowledge and an overview of a certain discipline and the particular tools it has to offer to assess a real-life case. However, it is simply impossible for any lecturer to master all disciplines in great detail. Therefore, an interdisciplinary team of lecturers designing and teaching the course is required. A major prerequisite for successful course design is that lecturers are able to make their disciplinary approaches *explicit* and are willing to *merge* their disciplinary insights. Only then, one arrives at a genuinely interdisciplinary assessment of the case central to the course. This is by no means an easy endeavour and, luckily, there are specific methods available for designing interdisciplinary education in teams (c.f. Vink et al, 2015).

REFERENCE LIST

[1] Aldrich, D.P. (2010). Fixing recovery: Social capital in post-crisis resilience. *Department of Political Science Publications,* paper 3, pp. 1-16.

[2] Comfort, L.K. (2007). Crisis management in hindsight: Cognition, communication, coordination, and control. *Public Administration Review, 67,* Issue Supplement s1, pp. 189-197.

[3] Davies, M. & Devlin, M. (2007). Interdisciplinary higher education: Implications for teaching and learning. Retrieved from the University of Melbourne, Centre for the study of education website: http://melbourne-cshe.unimelb.edu.au/resources/teaching-and-learning/curriculum-design/interdisciplinary-higher-education-implications-for-teaching-and-learning

[4] Federal Emergency Management Agency (n.d.). National Flood Insurance Program. Retrieved from https://www.fema.gov/national-flood-insurance-program

[5] Federal Emergency Management Agency (September 4, 2017). FEMA's national flood insurance program enhances the flood claims process and extends grace period for policy renewals. Release number: HQ-17-082. Retrieved from https://www.fema.gov/news-release/2017/09/04/femas-national-flood-insurance-program-enhances-flood-claims-process-and

[6] Klein, J. T. (2006). A platform for a shared discourse of interdisciplinary education. *Journal of Social Science Education, 5*(2), 10-18.

[7] Sebastian, T., Lendering, K., Kothuis, B., Brand, N., Jonkman, B., van Gelder, P., ... Nespeca, V. (2017). *Hurricane Harvey Report: A fact-finding effort in the direct aftermath of Hurricane Harvey in the Greater Houston Region.* Delft: Delft University Publishers.

[8] Shultz, J.M. & Galea, S. (2017, September 11). Mitigating the mental and physical health consequences of Hurricane Harvey. *Journal of American Medical Association.* DOI:10.1001/jama.2017.14618

[9]   Spelt, E. J., Biemans, H. J., Tobi, H., Luning, P. A., & Mulder, M. (2009). Teaching and learning in interdisciplinary higher education: A systematic review. *Educational Psychology Review*, *21*(4), 365.

[10] Rittel, H. W. J.& Webber, M. M. (1973). Dilemma's in a general theory of planning. *Policy Sciences, 4*(2), 155-169

[11] Vogler, J. S., Thompson, P., Davis, D. W., Mayfield, B. E., Finley, P. M., &Yasseri, D. (2017). The hard work of soft skills: Augmenting the project-based learning experience with interdisciplinary teamwork. *Instructional Science.* https://doi.org/10.1007/s11251-017-9438-9

[12] Vink S.C., Tartwijk van J., Bolk, J.H. &Verloop N. (2015), Integration of clinical and basic sciences in concept maps: a mixed-method study on teacher learning, *BMC Medical Education* 15(20).

[13] Western, J. (2016). What is *global* in global Security Studies? *Journal of Global Security Studies*, *1*(1), 99-101. DOI: 10.1093/jogss/ogv012

AUTHORS' BIOGRAPHY

Prof.dr. Bibi van den Berg, (1975) is full professor of Cybersecurity Governance at Leiden University, and the head of the Cybersecurity Governance research group at the Institute of Security and Global Affairs of this university. Van den Berg has an MA and PhD in philosophy, both from Erasmus University in Rotterdam. Her research and teaching focus on several themes: (1) cybersecurity governance, (2) governance of security and safety and (3) regulating human behavior through the use of technologies (techno-regulation and nudging. Van den Berg is the chair of ACCSS, the Academic Cyber Security Society in the Netherlands. She is also a member of the Dutch Cyber Security Council, a Council that advises the Dutch cabinet on how to improve cybersecurity in the Netherlands.

Dr. Ruth Prins, has a background in Public Administration and is employed as an Assistant Professor at Leiden University, Faculty of Governance and Global Affairs. She has published on the role of Dutch mayors in local safety networks, integrated safety policies in the Netherlands, policing in European metropolises and crisis management structures. In her current research projects, Ruth Prins focuses on mayors tackling various threats to public order, the national police force in the Netherlands, leadership and crisis, administrative approaches to organized crime and agenda setting for public safety governance. Since January 2020 she works as strategic advisor for security and safety to the municipality of Rotterdam in the Netherlands.