Brussels, November 22, 2019

Aleksandra Samonek

aleksandra.samonek@uclouvain.be
Institut supérieur de philosophie
Université catholique de Louvain
Place Cardinal Mercier 14, bte L3.06.01
1348 Louvain-la-Neuve

An interpellation for *Ethical Forum 2019* (December 5, 2019)

On the conflicts of values and inefficiencies in the cooperation between the academia and the national security institutions. Case study of cyber security
Please note that this is a draft not meant for circulation

1. Introduction

Some members of the academia, as well as some universities, may accept a position that "in peace-time the scientist belongs to humanity, in war-time he belongs to his fatherland", as Fritz Haber (1) was famously believed to have said. There are many arguments to support this claim, one of the most powerful being that winning the war is in the best interest of the community which sustains the academic institutions though funding for the public sector and, consequently, universities and their academic staff are obliged to contribute to the wartime effort of the community.

Some other academics and their institutions may believe that accepting *academic assistance in warfare* is not a valid position and that academic staff are at all times obliged to adopt a more humanist perspective, in particular that they should not facilitate the emergence of new or improved weapons and technologies of mass destruction. A strong argument behind this view is that academia's involvement in armed conflicts may give the community a temporary advantage, but a continuous commitment to peace allows for much more valuable benefits due to, among others, enhancing sustainability and stability of the legal and the economic system, increased protection of human rights and citizen's liberties and the development of the rule of law.

The two views, one of which I characterized as *academic assistance in warfare* and the other, which we may call *academic commitment to peace* in the form of rejecting the involvement in any wartime operations of the national security institutions (military, police, border police, militia, security and intelligence agencies, *etc*.), stand in direct conflict to each other during time of war and this conflict carries over to all forms of national security, including cyber security. But what becomes of the conflict during the time of peace?

A proponent of academic assistance in warfare may either extend their assistance for the time of peace, or conclude that, in the absence of direct threat to the community, their work towards the progress of the community must be resumed, even at the cost of strategic (political

1 Fritz Haber was a German chemist who accomplished the separation of nitrogen from air, creating compounds such as ammonia, chlorine gas, and Zyklon B of the gas chambers. However, it is estimated that more than half the human population of Earth is sustained by foods grown with fertilizers developed by Haber based on the same invention. For this accomplishment Haber received the Nobel Prize in chemistry in 1918, despite the fact that only three years earlier it had been used to kill thousands of allied soldiers in Belgium at the battles of Ypres.

or military) disadvantage to the country. Similarly, the proponent of academic commitment to peace may choose to assist national security institutions in a strive to sustain peace, help enforce the rule of law and social order, help fight crime, *etc*. Thus, it is important to see that the academic commitment to the national security institutions (or a lack thereof) made during the time of war may not carry onto the time of peace (and *vice versa*). However, although the war-time relations of academia to national security institutions have been present in the common social debate for a long time, the same cannot be said about their peace-time relations.

In this interpellation I would like to discuss some **problems related to peace-time relations between the academia and the national security institutions (NSIs)**, limiting myself to certain aspects of cyber security. In section 2, I point out certain inefficiencies which emerge from the cooperation between the academia, the private sector and the NSIs. I argue that many of those inefficiencies can only be eliminated at the cost of **violating core academic values** and discuss examples of values which constitute the social mission of the university in section 3. Finally, in section 4, I indicate the **financial and practical consequences** (to both academia and the society) of violating core academic values in the service of national security.

2. Inefficiencies

Be it peace-time or war-time, one of the problems in the partnership between the academia, the private sector and the NSIs is that **universities are rarely perceived as stakeholders** in the cooperation. To use the examples related to cyber security, academic involvement in the public institutions of expertise on cyber security is either purely symbolic, limited to reciprocal educational campaigns, or non-existent. A symbolic partnership is that of the European Union Agency for Network and Information Security (ENISA) and the academic sector. ENISA maintains a database of academic courses on issues related to network and information security(2) but, at least as far as is made public knowledge, the cooperation between the universities and the agency ends here. Moreover, much can be inferred from the fact that no further cooperation between the academia and ENISA is made public knowledge. In particular, the requirement of transparency obliges the universities to account for all partnerships which can benefit their social or educational mission. Since no such announcements are issued by the universities, it is safe to assume that in case of any involvement of academia (whether such involvement is the case or not) in the operations of ENISA has the form of a **service rather than a legitimate partnership**, and thus can be conducted in a covert manner.

Another example is that of the German Alliance for Cyber Security. In the mission statement of the Alliance (3) we find the following information:

The Alliance for Cyber Security is an initiative of the Federal Office for Information Security (BSI) founded in cooperation with the Federal Association for Information Technology, Telecommunications and New Media (BITKOM).

As an association of all major players in the field of cyber security in Germany, the mission of the Alliance is to increase cyber security in Germany and strengthen Germany's resistance to cyber-attacks. To do so, the Alliance for Cyber Security is building up a comprehensive knowledge base and supporting exchange of information and experience.

---

[2] Education map. A website featuring the contents of ENISA's database of academic courses and certification programs linked to Network and Information Security. URL: https://www.enisa.europa.eu/topics/cybersecurity-education/nis-in-education/universities (accessed: March 25, 2019).

[3] Information on Alliance for Cyber Security issued by the German Federal Office of Information Security. URL: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/ACS_Broschuere_en.pdf?__blob=publicationFile&v=4 (accessed: March 25, 2019).

So far, no university has been listed as a member of the Alliance, which in a rather obvious manner limits the access of the academic staff to the knowledge base and the information which are provided without limitations to the representatives of the private sector and the NSIs.

A thorough analysis of the academic-political situation in countries like, *e.g.*, the USA of the People's Republic of China is likely to further support the claim that universities are not considered to be stakeholders in their relation to the NSIs. However, it suffices here to observe the lack of influence of universities (and academics) on the national and European cyber security agendas and strategies within the EU to conclude that universities are treated as being in the service of the NSIs and not as a party in a mutually beneficial alliance (unless purely financial benefit for the universities is treated as priority).

Thus, in my opinion, an honest phrasing of the question about the peace-time cooperation between the academia and the NSIs is not whether the academia should partner up or collaborate with the NSIs, but rather whether academia should commence **providing service or assistance** to the NSIs for the **purposes specified by the NSIs and not the universities** or their staff. Even though other types of cooperation are possible from a purely logical point of view, it is crucial to keep in mind that they are not, in practice, made reality or even planned or pursued. As a result, universities assisting the NSIs during peace-time are in fact the source of workforce to the NSIs.

Regardless of our evaluation of the appropriateness of this arrangement, the problems which I discuss here arise from the fact that academic staff when involved in the assistance of the NSIs have to perform their tasks under a dual standard of accountability and work ethic. The first standard is that of strategic advantage over the adversary to the NSIs, for example over the agent attempting forgery, theft, an armed attack. The other standard stems from academia's commitment to education and social progress embodied in the commonly accepted academic values and via specific mission statements of the universities. One of the consequences of the latter standard is that of **transparency of research**, in particular the **obligation to publish the results** of research in an academic journal.

Siwei Lyu, an expert on image forgery detection, mentioned that one of the problems with staying ahead of the forgery technology is that most counter-forgery solutions are almost immediately made public knowledge via publication (4). On the other hand, the agents attempting forgery make sure to not publish (or even make publishable) their attack techniques and tools. As a result, in the field of image forgery detection, it often takes significantly less time to develop a successful attack method than to develop a method for detection or prevention. Similar remarks apply to other technologies and fields related to cyber security, perhaps most notably to cryptography. A crucial conclusion here is that as far as we employ academics to do NSIs' work, they remain bound by the fundamental standards of academic work and, as such, **academics are exceedingly inefficient as members of the intelligence workforce**.

In the following section (section 3) I describe further examples of core values which are potentially in conflict with efficient academic work in the service of NSIs. In section 4, I analyze one way out of this conundrum, that is, using the example just given, suppressing the publication of academic results which are of strategic importance to the NSIs or disregarding another core value of academic work. I argue that such decisions by the national governments

[4] Siwei Lyu, *The technical, societal, and cultural challenges that come with the rise of fake media*, The O'Reilly Data Show Podcast: Siwei Lyu on machine learning for digital media forensics and image synthesis. Interview by Ben Lorica, February 14, 2019. URL: https://www.oreilly.com/ideas/the-technical-societal-and-cultural-challenges-that-come-with-the-rise-of-fake-media (accessed: February 26, 2019).

have long lasting negative consequences, which sometimes far exceed the nation whose government had imposed secrecy on academic work. I demonstrate a few ways in which the violation of the core values could and in fact *has* resulted in strategic and economic failures, despite the fact that the problem of inefficiency of academic service to the NSIs was eliminated.

3. Conflicts of values

In this paper I make extensive use of the example of the conflict between the transparency of academic research with the bond of secrecy needed to maintain the efficiency of the academic service to the NSIs. However, transparency is by far not the only core academic value which can obstruct efficient academic service in the context of cyber security. Consider the following values (*cf*. University of Leeds (5) mission statement which represents a typical ethical commitment of a university):

- the commitment to the pursuit of truth,
- integrity, in particular openness, transparency and honesty,
- responsibility,
- academic excellence, in particular respecting academic freedom, encouraging critical independence, promoting creativity and new approaches to research and innovation within an ethical framework,
- community service, in particular public service and citizenship,
- inclusiveness, in particular equal opportunity and access to education and research.

4. Financial and strategic consequences of secrecy

4.1. Secrecy *vs* losses to public funds and academic workforce

The universities are established and funded from the national budget (either directly or indirectly) in order to provide a solid level of education and produce the results of research which contribute to social and economic progress. Take the suppression of publication as an example and consider the consequences to both, the society and the public funds assigned to the costs of education.

On one hand, when the results of research become unavailable, citizens and private businesses cannot make use of the tools which were developed due to public funding. For example, advanced image forgery detection tools could be available to the NSIs, but not the private financial institutions like banks and investment companies, even though (at least in theory) they contributed to the development of the results as major taxpayers. On the other hand, sharing the results with only a few major private initiatives (like is the case in Germany) is a clear indication of taxpayer discrimination and favoritism.

Then again, the costs of educating and sustaining a scientist are high compared to the rest of workforce. It is in the best interest of the community to use this hired worker in accomplishing tasks which cannot be performed by others. NSIs, in particular the military, is awarded a significant part of a typical national budget, quite unlike the higher education sector. Directing academic workforce towards military (and general NSIs) purposes further impairs the already unbalanced national budget. Whatever tasks are accomplished by the academic service in time of peace, NSIs can accomplish by training and hiring workforce of their own, which

5 *The University strategy, values and standards*. A public website of the University of Leeds. URL: http://hr.leeds.ac.uk/info/60/strategy_values_and_standards/229/the_university_strategy_values_and_standards (accessed: March 23, 2019).

will moreover be unconstrained by the standards of academic work and core values, and therefore more effective.

4.2. NSI funding and the polarization of the academic ecosystem

The NSIs may and often do try to alleviate their burden to the higher education sector by providing partial funding, thus removing only the workforce and results from the list of public benefits assets, but instead providing (partial or full) salary and funds for the research equipment and operations. This solution has an obvious and a non-obvious flaw.

The obvious flaw is that NSIs funding only makes up for a small part of the loss to the higher education sector. Many top scientists and the results their teams produce are being removed (often long-term or permanently) from the public domain. This means that for the taxpayers, the only way to make use of such results is to stay close enough to the NSIs to be made privy to the technological advancements worked out by the intercepted academic workforce. As a consequence, those agents who are close to the NSIs persist over those who enter the market too late, or do not have enough leverage to join the privileged circle of trusted taxpayers. In many ways, such strategies of redistribution of economic and strategic power resemble the functioning of feudal institutions.

In my opinion, a much less obvious flaw is the **polarization of the academic ecosystem induced by NSIs funding**. The disproportion of public funding between the higher education sector and the NSIs is large enough to lead to the situation in which a minor spending in the budget of a certain NSI (particularly the military) is a major contribution to the overall funding of the university as a whole, let alone a single department or research unit. Moreover, academic progress, including that in the domain of cyber security technology, is proportional to the resources and funding that the research unit is granted. When the military (or another NSI) fund the research of a unit at one university, but not others, it permanently disrupts the academic ecosystem. For one, other academic centers may at best hope for replicating part of the results produced by the massively funded unit involved with the NSI, a hope which will be further impaired by the draining of talent towards the funded unit. Then of course, whatever results they produce will be subject to the same censorship which involves the academic service at the NSI-funded university. Effectively, once the NSI decided to grant funding to the research unit of one of the universities, from a practical point of view, research units at other universities either must be redirected in their work, or disbanded altogether, as they are unlikely to be able to produce research of comparable quality and in any case, will be banned from publishing it.

4.3. Secrecy *vs* extensive economic and strategic losses

Based on the example of image forgery detection mentioned in section 2, we can easily estimate the relative cost of transparency in the form of making the technology and detection tools publicly known. Oddly enough, what is much more difficult to estimate (specifically in anticipation of the future development of technology) is **the cost of keeping the technology secret**. A well-known historical case is that of cryptography results in the post-WWII England.

After the construction of Colossus and breaking the German Lorenz cipher system during WWII, the English government made careful use of the intercepted and deciphered messages so as to avoid detection of their deciphering capabilities. All academic staff working in Bletchley Park (a British WWII center of cryptography and cryptoanalysis) were sworn to secrecy both during and post war. Moreover, all technology and tools developed during WWII in Bletchley Park were protected as a national secret. The strategy of the British government was to protect the deciphering technology while initiating the production of the machines using

the Lorenz cipher. The produced machines were to be sold to the foreign governments with the (obviously false) provision that the Lorenz cipher was not breakable. This strategy would allow England to covertly intercept and decipher all communications of foreign agencies which purchased the machines relying on Lorenz cipher.

At first glance, this decision may seem like a reasonable method to offset the huge costs of war-time functioning of Bletchley Park and gaining strategic advantage in the international relations. However, in the recent years it has become clear that in this case the costs of secrecy far outran the benefits. A few years ago, soon after the documents concerning the Bletchley Park technology were published, it became clear that the English government had in their hands most knowledge and technology needed for the development of the personal computer. The extent of capabilities accessible to the Bletchley experts was so large that, before the history of the discoveries was disclosed to the public, the general opinion was that the idea of constructing personal computer (or a *universal* machine with stored programs) was chronologically first conceived in the USA. As Copeland put it: "Historians who did not know of Colossus tended to assume quite wrongly that Turing and Newman inherited their vision of an electronic computer from the ENIAC group in the U.S." (6).

Consequently, by keeping all Bletchley technology a national secret, the British government stifled the development of its private sector and gave an immense economic and strategic advantage to the USA, an advantage visible in the fact that the USA is a global leader of hardware and software production, controls the global access to the world wide web and easily overshadows most European (and not just English) cyber security technology. In this sense, the strategic position of the entire EU has been shaped by a single decision of the national government to keep the technology secret. After all, whatever strategic and technological advantage England had not had, it could not bring to the table when it applied for EU membership in 1963, 1967 and 1969.

5. References

Siwei Lyu, *The technical, societal, and cultural challenges that come with the rise of fake media*, The O'Reilly Data Show Podcast: Siwei Lyu on machine learning for digital media forensics and image synthesis. Interview by Ben Lorica, February 14, 2019. URL: https://www.oreilly.com/ideas/the-technical-societal-and-cultural-challenges-that-come-with-the-rise-of-fake-media

The University strategy, values and standards. A public website of the University of Leeds. URL: http://hr.leeds.ac.uk/info/60/strategy_values_and_standards/229/the_university_strategy_values_and_standards (accessed: March 23, 2019).

B. Jack Copeland, *Colossus: Breaking the German 'Tunny' Code at Bletchley Park. An Illustrated History*. URL: http://www.rutherfordjournal.org/article030109.html (accessed: March 27, 2019).

Education map. A website featuring the contents of ENISA's database of academic courses and certification programs linked to Network and Information Security. URL: https://www.enisa.europa.eu/topics/cybersecurity-education/nis-in-education/universities (accessed: March 25, 2019).

Information on Alliance for Cyber Security issued by the German Federal Office of Information Security. URL: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/ACS_Broschuere_en.pdf?__blob=publicationFile&v=4 (accessed: March 25, 2019).

6 B. Jack Copeland, *Colossus: Breaking the German 'Tunny' Code at Bletchley Park. An Illustrated History*. URL: http://www.rutherfordjournal.org/article030109.html (accessed: March 27, 2019).