CCDCOE

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

Corinne J.N. Cath, Ludovica Glorioso, Maria Rosaria Taddeo

NATO CCD COE Workshop on 'Ethics and Policies for Cyber Warfare' (Magdalen College, Oxford)

Report

Tallinn 2015

www.ccdcoe.org
publications@ccdcoe.org

Contents

Summary

The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) workshop on 'Ethics and Policies for Cyber Warfare' took place on 11-12 November 2014 at Magdalen College, Oxford. It brought together 10 distinguished experts from the United Kingdom, the United States, Germany, Spain, Italy, the Netherlands, Norway, and Estonia, gathering representatives from academia and from international organisations such as the European Union, the United Nations Institute of Disarmament Research, the Cyber Security Centre in Oxford, and Oxford University. The workshop was chaired by Dr. Mariarosaria Taddeo and Lieutenant Ludovica Glorioso and was the second of its kind organised by the NATO CCD COE.

The first workshop on ethics of cyber conflict was held in Italy at the Centre for High Defence Studies (CASD), in November 2013. The proceedings of the presentations are available at NATO CCD COE's website (https://ccdcoe.org/multimedia/workshop-ethics-cyber-conflict-proceedings) and reflect ideas related to the ethical aspects of a number of issues such as the 'Just War Theory' in cyber conflict, cyber warfare, cyber espionage and the status of cyber combatants, and the ethical basis of law.

Consistent with the approach of the previous event, to have an arena of discussion on the legal, ethical, and technical issues of cyber warfare, the workshop in Oxford was organised to allow speakers from three interacting fields – politics, law and cyber security – to develop their views about the existing regulatory gaps in cyber warfare and its ethical underpinnings. Each of the speakers dealt with the issues surrounding the definition of cyber warfare and the practical consequences of their definition for filling the regulatory gaps. This report will present the views as given by those experts and identify the recommendations made.

The first part, Politics, began with a discussion of the extent to which current international structures are able to develop cyber security norms, and continued focusing on the possible ways in which these issues can be addressed by international bodies, considering their limited mandates for addressing the international security aspects of cyber interaction. In general, the work of United Nations Group of Governmental Experts (UNGGE) and the conclusions of the NATO CCD COE in the form of the Tallinn Manual on the International Law Applicable to Cyber Warfare were acknowledged and regarded as a confirmation of the intent of nations to remain bound to the existing legal, political and ethical frameworks for warfare. The discussion moved to assessing in what way exactly the international legal norms of warfare can be applied to cyber warfare. This illustrated the lack of consensus amongst the participants, some holding that the current international legal framework is able to regulate cyberspace efficiently as we develop better fitting systems, while others argued that cyber warfare is a radical and new phenomenon which brings a need for new frameworks. Two specific political obstacles to filling the current regulatory gap were highlighted: (i) the fact that cyber does not fit our post-Cold War structured world of nation-states and international bodies, and (ii) the hyper-connectivity associated with cyber, which prompts the need for policy-makers to focus more on the interconnectedness of the different issues at stake instead of their compartmentalised

uniqueness, as well as to adapt to the fact that policies constantly lag behind technological developments.

The discussion focused on efforts to find a set of common norms or a shared approach towards cyber warfare in the international community. The experts debated the difficulties of developing a set of shared ethical principles when dealing with diverse political actors and entities. They also discussed the problems arising from the lack of a commonly accepted definition of cyber warfare and the limited ability of the international community to contain any potential forms of cyber warfare.

The central conclusion focused on the need to develop a consensus on a unified set of norms from which new principles can be derived, and into which old ones can be integrated, so as to manage cyber warfare. In particular, the need was emphasised for nation-states and international bodies to engage with a wide range of actors seeking consensus on what are acceptable cyber warfare practices. The need to develop an adequate definition of 'cyber weapon' was also identified, and it was argued that this definition could help advance international understanding of what constitutes cyber warfare and to what rules it should adhere.

The second part of the workshop focused on the law and examined the applicability of current legal mechanisms of warfare to cyberspace, looking specifically at the issues of deterrence, proportionality, perfidy, and casus belli. Improved transparency and attribution mechanisms were also identified as important aspects in developing morally sound and effective norms for cyber warfare. The speakers agreed on the need to work with existing legal and regulatory structures until a better fit, or an entirely new set of rules, could be developed (if at all). They had different perspectives, some speakers arguing that cyberspace is pre-political, and therefore pre-ethical, and thus prior to the application of public policy discourse to it, cyber space needs to be constituted as a political space. Deterrence was offered as a possibility for guiding this process.

The analysis of perfidy and cyber attacks as a casus belli focused on the implications of the non-physicality of cyber warfare in applying concepts like perfidy and others of Just War Theory to the case of cyber warfare. The speakers focused on the distinctive nature of cyber warfare, distinguishing it from regular warfare and concluding that we should re-evaluate how we understand cyber warfare strategies and assess their consequences.

The third section focused on the role and contribution of experts from academia in filling the regulatory gaps in cyber warfare. This question was examined using a multi-disciplinary approach, bringing together the various fields of expertise of the speakers. As with the previous discussions, much of the focus lay with the lack of a coherent definition of cyberspace. The speakers agreed on the need for such a definition to advance the discussion, but differed in their opinions on how to formulate it. The delegates looked at different mechanisms for developing ethical norms, universal principles that could be applied to cyber warfare and gave their views on the usefulness of Just War Theory, information warfare and a meta-level rule of law to develop ethical norms to regulate cyberspace. One possible solution proposed was to extend the scope

of the moral scenario to include informational objects, as they have an increasingly important role in the functioning of our societies. The experts stressed the need for an inclusive approach, encompassing the different stakeholders affected by cyber warfare and accounting for the networked nature of the cybersphere, to fill the current ethical regulatory gap surrounding this phenomenon.

Political Section – Summary

In this section the discussion focused on the difficulties of defining cyber warfare within the international community and the subsequent issues surrounding regulation and norm development for cyber warfare.

When discussing the regulatory gap concerning cyber warfare and the ethical problems underpinning it, it was argued that many of the issues spring from the divergent views on cyber warfare held by different international actors. This lack of consensus on an international level, caused by diverging needs, interests and cultures, complicates our ability to define cyber warfare and to justify the ethical norms that should guide it.

At the same time, the nature of cyberspace itself complicates any attempts to find a common definition. Cyberspace is a fast-changing environment that brings together a multitude of actors beyond those traditionally involved in setting the regulatory agenda for warfare. The technological development of cyberspace is also affected by the constant strain of physical geo-political events, which also influence the power dynamics in cyberspace. It is becoming increasingly difficult to define cyber warfare, and the ethical principles that should guide it, through consensus between sovereign entities that act in different international and multi-national bodies.

Although the debate over the definition of cyber warfare was not settled at this conference, and the experts' opinions on the nature of cyber warfare differed, there was general consensus that cyber is sufficiently different to warrant a definition that goes beyond putting the prefix 'cyber' before the word 'warfare'. One of the definitions that pointed out the unique nature of this type of warfare focused on its ability to render transparent what was once opaque. Another definition given during the conference focused on the difference between cyberspace as a location compared to physical space, emphasising that cyberspace is man-made, privately owned, and mainly used by civilians. These definitions led to an interesting debate on the nature of the cyberspace.

It was also suggested that we move beyond the term 'cyber warfare' as it is invokes an image of trenches and bunkers, which makes cyber seem like an isolated phenomenon. This was explained as being both untrue and unhelpful, because it misses the crucial point that one of the defining elements of cyberspace is its interconnectivity. According to one expert, this meant that we are all now just as strong as our weakest link. This scenario poses the need for an approach to the regulation of international relations different from the one developed during the post-Cold War period. Another possible solution presented by the experts focused on the need for the international community to interact with a wider range of stakeholders, including those that would normally not have been part of the discussion. Efforts should be made not just to define cyber warfare but also to reach an internationally supported consensus on what the implications of this definition are for the norms and rules of cyber warfare. It was also stressed that the search for consensus needs to account for multi-national as well as multi-stakeholder views, including academia, citizens, netizens, corporations, and other internet stakeholders. It is clear that cyber warfare is not an isolated phenomenon: it

connects many different political, economic, social and military spheres. Hence, any definition needs to be determined using a multi-stakeholder approach.

During the discussion it was mentioned that a possible way to deal with contention in cyberspace – awaiting a solid definition of cyber warfare – would be to develop consensus regarding the definition of the term 'cyber weapon'. This definition is particularly important because it is a necessary prerequisite for nation states to adequately apply international humanitarian law and develop future ethical norms for cyber warfare. It was argued that defining cyber weapon as a concept would be a solid initial step towards reaching a larger consensus.

A more political realist view of the situation would involve a partial acceptance that, at least under the status quo, it is not feasible to prevent cyber warfare. We should therefore focus our energy on developing means of guaranteeing a sense of cyber stability. This stability refers to the ebbs and flows of what is going on in the world, mapping existing conflicts. If we are unable to prevent cyber warfare then perhaps we should focus our efforts on ensuring that inter- and intra-state conflicts in cyberspace cannot trigger kinetic warfare in the physical world.

Participants provided examples of areas where common ground on cyber warfare norms could be found. Two of the areas repeatedly proposed were existing International Humanitarian Law, and forums for multinational discussion such as the United Nations. It became clear that there is a tension in cyberspace resulting from the fact that the lack of definition both helps and hinders the ability of different political actors to leverage this newfound space of international relations.

Law Section – Summary

The second part of the conference investigated the relevance of existing legal mechanisms of warfare to cyberspace. Special attention was paid to deterrence, proportionality, perfidy and casus belli. Increased transparency and improving attribution were identified as vital to developing ethical norms for cyber warfare.

The discussion started with recognition of the importance of the United Nations Group of Governmental Experts' (UNGGE) consensus that International Law applies to cyberspace. According to some experts, this should be seen as a confirmation of the intent of countries to remain bound to the existing legal, political and ethical frameworks for warfare, whether it refers to kinetic or cyber action. The perspectives on these issues were clearly informed by the professional and academic backgrounds of the various speakers.

Building on this, it was proposed that an alternative approach to developing an ethical framework for cyber warfare could be based on existing legal structures. The experts critically discussed the validity of a system that was not created with 'cyber' in mind, because it complicates application of the existing system to a digitised world. One expert asserted that laws of targeting apply in their current form, which involves the principles of distinction and proportionality and the duty to take precautions when conducting an attack. Another expert mentioned that we need to be careful when employing analogies between kinetic and cyber warfare. Instead of fighting the new implications of this type of warfare, we need to start focusing on devising solutions to deal with them. A consensus was reached that, for the sake of practicality, pressing cyber warfare issues should be addressed using existing legal framework however imperfect their fit to the new situation. The preference for a faulty system over no system is based on the assumption that if the alternative is a cyber 'Wild West' in which actors perceive they are not bound by any of the rules associated with traditional warfare, a flawed system is preferred to none at all. As one expert pointed out using the example of Stuxnet, unregulated cyber actions often not only harm the intended military, but also end up heavily damaging civilian infrastructures.

As the discussion continued, it became clear that using existing legal frameworks as the basis for filling regulatory gaps in cyber warfare raises more questions than it answers. Some of the main questions were related to the way in which the impact of actions of cyber warfare should be measured. Several options for measurement were offered. Certain experts argued for an effects-based approach, where an attempt is made to measure the impact of an attack using indicators associated with kinetic warfare, such as civilian casualties and proportionality. Others argued for an approach that examines the methods used by the cyber-attackers, because as cyber attacks are non-physical, many of the standard theories of casus belli are less applicable and states are too easily enticed to engage in unilateral defensive responses to perceived cyber attacks. An alternative possibility would be to combine the two approaches. A particular issue surrounding the UNGGE consensus is that the report does not contain a specific definition of how international law should apply to cyber warfare. This gap became particularly clear in the discussion about the applicability of the concepts of deterrence,

proportionality and perfidy in cyber warfare. Nevertheless the principles of proportionality and perfidy were subject to Tallinn Manual research and are addressed in the book.

Deterrence and Proportionality

Participants provided examples of areas where common ground on cyber norms might be found. One of those areas repeatedly proposed was deterrence. Although it does not provide a solid guarantee of cyber peace, it is a principle that has the potential to unify different actors and build further consensus.

According to the experts, the main problem we face is the way in which we can make cyberspace subject to the ethical, political and legal rules of warfare as they pertain to kinetic action. One of the possible solutions to this conundrum is adapting the concept of deterrence to cyberspace by assessing an adversary´s most valuable assets and threatening those with attack, as is done with nuclear deterrence. This requires a recalibration of what constitutes prized assets in cyberspace. One expert argued this could be done when cyber assets such as anonymity, deniability, uncertainty, and culpability are turned into liabilities. The idea of deterrence by association was introduced: if attackers can be associated with a cyber attack they will be less inclined to execute it. The fear for reputational damage and sanctions which might follow from being associated with an attack could work as a cyber deterrent, stressing the need for the development of international norms that would make highly disadvantageous for any state to take part in a cyber attack. Another expert argued that conflict in cyberspace, like the possibility of nuclear warfare in the sixties, is transforming military strategy. The Cold War era led to a shift from the science of military strategy to game theory. Cyber war could change this paradigm again by moving game theory to a situation of 'blue war': the threat and gradual occurrence of public and proportionate cyber attacks to resolve disputes between nations without an all-out escalation of violence. In this scenario, a digital arms race is inevitable; but it might also have many positive effects in terms of new technological spin-offs. This particular scenario, for the time being, remains to be paired with conventional kinetic and nuclear deterrence, as societies are not (yet) fully dependent for their functioning on ICT.

Proportionality was also highlighted as a useful concept to regulate cyber warfare. Again, the problem identified by the experts concerned its applicability to the case of cyber warfare. In order to apply this particular principle two parameters need to be weighed: the expected incidental damage to civilians and civilian objects on one side, and the anticipated concrete and direct military advantage on the other. It was in the weighing of these two that the experts and participants diverged on the practical usefulness of this concept. The main problems in this discussion centred on defining incidental damage and military advantage in a cyber scenario. In addition, the question was raised of what to do about non-violent military attacks, because non-violent attacks are not sufficient to trigger the application of the law of targeting under the Geneva Additional Protocol I. Some experts argued that this does not raise a substantial issue, as the civilian damage in cyber attacks is potentially less harmful to civilians

because it involves less loss of life. Others argued that cyber attacks are potentially more dangerous because, by default, they involve civilian infrastructure. Taking into account society's dependency on information technology, we need to recognise that it has become possible to do significant harm through non-destructive means. A third group argued that incidental damage and military advantage are good examples of the 'unknown unknowns'. There are too many undetermined variables involved in cyber attacks to make a good prediction of these two parameters.

The discussion on deterrence also prompted a debate on retaliation for and escalation of a cyber attack. The question in this case was whether a cyber attack could trigger a kinetic response, and if so what guidelines should regulate such a scenario. During the discussion it was argued that the answer to these questions can be found in the U.N. Charter and hinges on the extent to which an attack is proportionate.

The discussion on proportionality and retaliation also prompted a debate on the need to reconsider the definition of the concepts of violence, harm, and attack so as to incorporate the ways in which new technology has enabled us to cause damage by, for example, limiting or removing functionality. The Tallinn Manual, which was mentioned often as a good foundation on which to build our understanding of cyber warfare, does not include functionality loss as an attack in the sense of the law of armed conflict. One of the participants gave the example of a cyber attack leading to functionality loss of the energy grid.

Perfidy and dual use

Discussing perfidy – the illegal act of military forces impersonating civilians in time of war – brought out some of the difficulties in measuring the impact of cyber attacks. The experts agreed that perfidy was seen as a measure through which to regulate cyber warfare. The discussion focused on the strategic role of perfidy in war, and its potential role in cyber warfare. Perfidy in kinetic warfare is considered a breach of the laws of war. Yet, in cyber warfare, those engaging in the attack often see perfidy as a necessary evil. One expert detailed that, common belief notwithstanding, computers are relatively resistant to manipulation. This means that the best hope for a successful attack lies in preventing computers from recognising the attacker – which, it can be argued, is perfidy. Dual use in cyber warfare also emerged as a key problematic point. All speakers agreed that dual-use targets should not be considered legitimate military targets. There is a clear need to define norms that would ensure proper identification of targets, the acknowledgement of the attack, the creation of cyber havens, and rules and norms to ensure attacks are proportionate. This last issue was the source of disagreement amongst the speakers and led to a broader discussion on attribution and transparency. Some speakers argued in favour of enhanced transparency, on the basis that it might deter the attackers for fear of retaliation, others that increased transparency also increases the information about attacks that might be used for improving the impact of existing cyber attacks.

Attribution and transparency

Attribution and transparency in attacks are important in kinetic warfare, but their place and role in cyber warfare is less well established. Attribution is particularly complicated due to the nature of cyber attacks. The experts argued that attribution is important in order to apply ethical rules to cyber warfare because, without it, it is unclear to whom rules, and sometimes penalties, should be applied. During this discussion, several specific issues were mentioned that countered the assumption that attribution is important. The first focused on the fact that attribution in the physical world is often not as straightforward as assumed; examples of the current conflict in Ukraine were mentioned.

The debate on attribution turned out to be closely linked to the question of transparency. Some experts argued that there needs to be more transparency surrounding cyber attacks, others that increased transparency has several negative side-effects. Those arguing in favour of increased transparency held that it was a necessary requirement in order to make cyberspace political, in the sense that it is seen as a legitimate space where political, legal, and ethical norms and rules apply. This point was the source of much discussion, as some of the experts and participants argued against transparency over attacks – mainly to ensure that cyber criminals did not abuse the code of attack vehicles, as it was the case with the leaked Stuxnet code.

In the closing round-table session, the experts and participants maintained that common ground to shape ethical principles for cyber warfare can be found in existing International Humanitarian Law. There was consensus amongst the experts that even if cyber warfare could be construed as a new phenomenon, this does not imply that current laws do not apply. There is a clear need to work with the current legislative framework and build from there. In this process it will become clear which laws can be applied to cyberspace, which need to be adapted, and which must be created anew.

Academia Section – Summary

The third session of the workshop addressed the role of academia in developing solutions to the regulatory gaps and lack of ethical standards. The experts described how, where, and by whom solutions should be developed, what the main obstacles were, and what were the possible options for going forward.

Panellists and participants agreed that the traditional governance entities, such as the nation-state and international bodies, such as the United Nations, dominate the development of regulations and ethical norms guiding cyber warfare. However, the increased influence of the private sector and the need for cooperation between different types of stakeholders was also recognised. The experts identified several issues facing the development of an ethical framework for cyber warfare.

A specific issue was the problem of the lack of a shared understanding of what cyberspace is. Several of the experts proposed the development of a model that would allow decision-makers to use the same reference point and compare different considerations so as to guide stake-holders to make a fair decision based on a shared understanding of the problem. This model would bring together different stakeholders, and approach cyber attack from a holistic perspective. Although the panellists agreed that the model brought together different views highlighting the circumstances in which miscommunication about cyber issues arises, there was some concern over the practical applicability of this model. In particular, one participant argued that the problem with the model was that it was created without taking into consideration the needs of the individuals it is intended to support. It assumes that key actors in the debate on cyber attacks have a clear stake in developing strong ethical norms, which is not always the case. Cyber attackers also benefit from the lack of a consolidated set of norms and rules, and political actors benefit from pushing their particular definition. It is this ideological divide that has been limiting the development of a global consensus. Considering alternative models for guiding cyberspace, although not always politically feasible, could produce interesting results and novel approaches that might benefit the discussion.

Another issue that was considered was the need to develop a better understanding of how Just War Theory can be applied to cyber attacks. One of the participants argued that we should be careful when trying to force new phenomena to fit old paradigms. The analogy of pushing square pegs into round holes was repeatedly mentioned, and it was argued that if we attempt to force cyber warfare into the shapes we readily recognise, we might not be doing justice to the complicated nature of this issue. Some practical examples of this were discussed. For instance, the questions of when a cyber attack can be considered a use of force, and when a cyber operation amounts to an armed attack arose, especially as many aspects of such an attack will be intangible and hence difficult to quantify.

There was general agreement that Just War Theory is still a good framework for regulating war, including cyber war. But as Just War Theory presupposes knowledge of identities, intentions and trust, there is a clear need to update it to the cyber era in

which we live, as identities, intentions and trust are not necessarily transparent in cyber warfare. One of the possible solutions presented was to approach Just War Theory as a necessary but not sufficient instrument in developing norms for cyber warfare. It was argued that to develop a suitable ethical framework for analysis of cyber warfare, Just War Theory needs to be merged with Information Ethics so as to expand the scope of the analysis and regulation to include also the cyber realm, artificial agents and intangible objects.

The existence of a hiatus between the ontology of the entities involved in traditional warfare and those involved in cyber warfare was stressed. As a consequence of the hiatus, it was argued that Just War Theory does not provide the sufficient conceptual tools to regulate cyber warfare, hence posing the need for the development of an ethical set of guidelines that can simultaneously weigh cyber risks, rights associated with information technology, and issues of determining responsibility for actions of cyber warfare.

It was also stressed that, with the so-called information revolution, some of the pivotal categories used in regulating society, such as private vs public, military vs civilian, are being reshaped and the very distinction between such categories is blurring. Warfare provides a particularly clear example of how lines become blurred as information technologies are increasingly used to deliver military strategy. The theatre of war has moved online, where attacks are aimed at physical and non-physical targets and increasingly focused on disrupting the critical ICT structures of enemies. This type of warfare merges the non-physical domain, often associated with attacks on digital agents and targets and low levels of violence, with the physical domain which focuses on attacking physical targets and agents and has high levels of violence. In this context, the discussion focused once more on the definition of cyber attack and on the requirements that it needs to meet to qualify as a use of force or an armed attack. Disagreement amongst the participants and experts on how to define this remained unresolved. However, by focusing on the disconnect between the current tests, laws and ethical frameworks that focus on the definition of war as physical and violent, and the current technological capabilities of cyber warfare, steps were made towards bridging the regulatory and ethical gaps.

Conclusions

The session ended with a call to action for the experts and panellists to ensure that the conversations about these important topics continue beyond the workshop. In particular, emphasis was put on the importance of ensuring that the development of a solution to the current regulatory gap in cyber warfare, and the ethical issues underpinning it, is developed in an interdisciplinary way and involves all stakeholders; a networked problem can only be addressed in a networked fashion. Participants and experts agreed that there was an increased need for dialogue between the stakeholders involved in cyberspace. At the moment, there are too few opportunities for discussion where governments, legal scholars, and public and private sectors are all represented. This event offered one such occasion and should be seen as a step in the right direction; however, many more such steps need to be taken in order to address some of our time's most pressing issues concerning cyber warfare.