International Law and Cyber Warfare
An agenda for future research

Dr Bela Bonita Chatterjee
Lancaster University Law School/Security Lancaster
Contents

3.....Guest Preface: Professor James A. Sweeney
4.....Executive Summary
7.....Section 1: Background to and rationale for Workshop: Why cyber warfare and international law?
18...Section 2: Methodology and Structure of the Workshop
20...Section 3: Proceedings of the Workshop
26...Section 4: Conclusions: An agenda for future research
29...Section 5: Key legal documents and cases, glossary and bibliography
36...References
40...Appendix: Figure 2 source data
Endpapers: Author Bio and Conference Confederates, acknowledgements
Guest Preface: Professor James A. Sweeney

I had the great privilege of observing and assisting the drafting of the Tallinn Manual, in my capacity as rapporteur for the project in its early stages. The present workshop and its resulting report are a welcome effort to move the agenda onwards and outwards.

The report identifies four principles and six very constructive suggestions for further development in this vital field of inter-disciplinary study. It is vital because it challenges core spatial and temporal notions of conflict, requiring us to reason again from first principles how this new form of conflict be recognised and regulated. It is inter-disciplinary not least of all because of the combined legal, ethical and technical issues presented. To some extent this is reflective of continuing debates on emerging means and methods of warfare, asymmetry, non-state actors, and human rights in conflict zones. But other aspects may be truly unique, and that is where workshops such as the one giving rise to this report may provide real insights.

Professor James A. Sweeney, Lancaster, March 2014.
Executive Summary

Reports that we are under cyber attack are now commonplace. The American Military has recently reclassified a number of cyber security tools as ‘weapons grade’, underlining the legitimacy of software as weaponry in its own right.¹ Cyber weaponry seems to evolve as rapidly as it spreads. The ‘Flame’ Malware that was identified by Kaspersky Lab as deleting sensitive files in the Middle East is believed to dwarf its infamous predecessor, Stuxnet, which was targeted at Iranian nuclear facilities.² In short, in the digital age, kinetic warfare may no longer be the main vector of attack upon the Nation State and any defence strategy will likewise need to consider digital means of resistance and retaliation.

In the UK, cyber attacks have been characterised as a Tier One threat to national security, and policy is now developing around the best ways to implement cyber warfare capability and resistance, as witnessed most recently by the establishment of a Defence Cyber Security Programme and the allocation of £860 million to strengthen cyber capacity.³ Internationally, other military powers such as America, Australia, Canada and Russia are now starting to articulate their stance towards this sphere of operations.⁴

Against this background, the role of law - international law in particular – is perceived as critical in establishing the ground rules for conduct in cyber warfare. Particular questions focus on what might legally permit a country to initiate cyber operations, and the law applicable once initiated. Yet the legal framework within which any military/policy response must be orchestrated is arguably underdeveloped in appreciating the specific dangers and demands of online hostilities. International legal norms were formulated prior to the emergence of cyber warfare, and no treaty provisions address it directly.⁵ The publication of the Tallinn Manual on the International Law Applicable to Cyber Warfare in 2013 (hereinafter “the Tallinn Manual”), produced by an independent international group of experts at the invitation of NATO, has been a welcome initial step in developing legal guidance in this area.⁶ However, it lacks the authority of a legal instrument, representing only the drafters’ personal and private viewpoints, and the scholarly field is comparatively underdeveloped in relation to the importance of the topic.

The alignment of these four factors – (1) The heightened public profile of cyber warfare, (2) The increasingly open acknowledgement of cyber warfare at International level (3) Legal uncertainty and (4) the publication of the Tallinn Manual – prompted Security Lancaster to organise an interdisciplinary Workshop with Security Lancaster academics and attendees from a wide range of MoD establishments on the future of International Law and cyber warfare. Particularly given the embryonic nature of the field, our Workshop offered an early opportunity to draw together military, legal, international relations and security expertise with the aim of mapping an agenda for future legal research that would be of maximum relevance to key stakeholders.

At an exploratory Workshop, the initial questions set were framed in a broad manner so as to expose and explore potential key issues relating to the adequacy and relevance of the legal framework envisaged by the Tallinn Manual: Was it sufficiently comprehensive from a military and legal perspective in its coverage of cyber warfare to contribute to the
planning and conduct of military operations? Did it go far enough in its guidance and if it fell short, where could it be developed? What alternative positions might be taken that had not been envisaged by the Tallinn Manual?

The resulting discussion, enriched by the different fields of expertise around the table, led us to different points of inquiry not initially envisaged by our opening set of questions. This was helpful in causing us to critically reflect on our approaches to the field and enabling us to identify where more pertinent questions lay (not necessarily, as it turned out, in the field of international law). As far as these emergent topics of interest were concerned, although there was not always a clear consensus amongst the delegates, we could distil a number of key questions and findings from the Workshop. These can be summarised by four underlying principles and six key areas of interest which we suggest form the basis of a future research agenda:

Four Underlying Principles

1. The concept of war as symmetrical State-on-State conflict needs challenging. Although the Tallinn Manual considers international law and thus focuses primarily (although not exclusively) on States, we suggest that the principal belligerents in cyber warfare are unlikely to be States themselves, and the role of non-State actors in particular is unlikely to be adequately addressed by a focus on international law and the use of force paradigm alone.

2. Linked with principle 1, a more holistic approach to legal research is needed if research on cyber warfare is to reflect the complex reality of cyber operations. In particular the interplay between international and domestic law needs to be more extensively considered to reflect the hazy boundaries between States, non-State actors and the criminal fraternity.

3. A focus on cyber ‘peacekeeping’ might be as productive as a focus on cyber war – a promising channel of investigation opens up regarding the role of cyber intervention in weak/unstable States and the legality of such intervention.

4. The lexicon of cyber warfare needs careful thought, and key terminology needs to be defined and considered in its particular context. Multiple valences need to be articulated as clearly as possible if interdisciplinary/contextual work is to be conducted.

Six areas for development:

- What is/should be the legal approach to cyber warfare conducted by non-State actors and/or federated/balkanised networks, and what liabilities and obligations might lie with non-State actors more widely in relation to cyber weaponry and critical digital infrastructure?
- How should the ‘attack’ of cyber offensives be conceptualised within the Law of Armed Conflict? Should the conceptual framework of kinetic attack be extended by analogy?
- What legal questions emerge from the manipulation of social media networks etc. to de-escalate situations of tension in weak/unstable States?
- What personal or other liabilities might flow from combatants’ reliance on information streams produced by software provided by private suppliers/coalition partners?
- Is there a duty of ‘digital decontamination and reconstruction’ regarding cyber operations?
- What is the scope of the duty of care regarding cyber operations and by whom is it owed?

As our Workshop made evident, more research needs to be done in the area, but our identification of key questions is an essential precursor to this process.
Structure of the report

The report is structured in five sections. The first section aims to contextualise the Workshop and findings by mapping out in some detail the factors which prompted us to come together for dialogue, namely the heightened profile of cyber warfare, the increasingly open acknowledgement of cyber warfare at international level, legal uncertainty and the publication of the Tallinn Manual. The second section describes the methodology and structure of the Workshop. The third section details the proceedings of the Workshop, describing how the debates developed. The fourth section summarises the results, outlining our suggested agenda for moving forwards. The fifth section provides a glossary of key terms and concepts related to the report, plus a list of sources.
Cyber warfare and international law: An agenda for future research

Section 1: Background to and rationale for the Workshop

Why cyber warfare and international law?

What led us to hold a Workshop on cyber warfare and international law? We identified four factors, the coalescence of which provided our rationale; (1) The heightened public profile of cyber warfare (2) The increasingly open acknowledgement of cyber warfare at International level (3) Legal uncertainty and (4) the publication of the Tallinn Manual. These factors are discussed below:

1) The heightened public profile of cyber warfare

Cyber warfare has long been a staple theme of science fiction. Early films such as War Games and Terminator depict a dystopian future where cyberspace is a theatre of conflict and computers herald the destruction of mankind. Yet as online capability has developed in the last few decades, cyber warfare has started to move from fantasy to reality, coming to be perceived as not only a credible but escalating threat. Cyberspace represents a potential new man-made theatre for war that not only sits alongside the existing arenas of land, air, sea and outer space but also interconnects with them.7

The term 'cyber warfare' is not a legal term of art or a political concept with a universally agreed definition – a problem considered in detail in section 2 - but it may generally be understood to refer to the hostile use of Malware, which is software implemented for the purpose of disrupting the correct operation of computer and network-based systems.8 There are debates as to when the first ‘official’ incident of cyber warfare occurred - a Russian pipeline explosion in 1982, allegedly caused by Malware inserted into the pipeline’s control software, has been cited as an early example. However, there are doubts as to the veracity of the account.9

A more generally agreed timeline starts to develop from around 2007, with cyber operations directed at Syria and Estonia. This incident involved disruption to Syria’s entire radar system to coincide with a conventional air attack by Israel. Whilst connected with a kinetic operation, the event demonstrated that digital manoeuvres could be an important part of a State’s military capabilities.10 A second and more renowned incident was where Estonia, a country highly developed in terms of digital infrastructure, suffered a prolonged and organised Distributed Denial of Service (DDoS) attack as well as spam and website defacement. Although unconfirmed due to lack of evidence and official denial of involvement, suspicion centred on Russia as the originator.11 The event was significant in that it was apparently unconnected with a kinetic attack and thus a purely cyber operation.
In the following year, digital attacks on Georgian websites coincided with a traditional military conflict between Russia over territory in South Ossetia. The attacks included the defacement of key national web pages, DoS attacks on media, public and private sector sites, and the use of Malware to intensify and accelerate the attacks. 2009 saw co-ordinated DoS attacks against government, media and financial web pages in America and South Korea and in 2010, Stuxnet, considered at present to be the apex of cyber warfare, was targeted at Iranian nuclear facilities with the reported effect of physically damaging their operation.

Stuxnet was a watershed moment in terms of the development of cyber warfare due to its kinetic effect against a State’s critical national infrastructure and the sheer sophistication of its programming, strongly and widely believed to have been originated by Israel in association with America. Since Stuxnet, reports of digital attacks have developed apace against various corporate, military and State targets to encompass such activities as IP theft, spying, hacking, DDoS attacks and web defacement, although such attacks may not necessarily coincide with kinetic military action.

Like nuclear proliferation before it, the public profile of cyber warfare – as part of a wider debate on cyber security - has now become raised to an extent where it is difficult to escape mention of it on a regular basis. Some recent press reports are illustrative of the phenomenon: The Information Age reports that

“the US Air Force has classified a number of cyber security tools as weapons so that its cyber warfare programmes are more likely to win government funding...this means that the game-changing capability that cyber is, is going to get more attention and the recognition that it deserves.”

The Telegraph writes of ‘cyber warfare and the new age battleground’, stating that:

‘cyber warfare is being played out right now, in very ordinary-looking offices, in very ordinary countries, around the world’.

The New Republic reports that the media itself has been a target, as seen through the ‘Syrian Electronic Army’, an online collective of hackers allegedly aligned with the Assad regime, hijacking of a number of prominent news sites and information streams including the New York Times, Financial Times, Twitter and Facebook to spread disinformation about the Syrian conflict. Meanwhile, Wired describes a secret Pentagon project that would make ‘cyberwar as easy as ‘Angry Birds’ whilst Vanity Fair reports that:

‘on the hidden battlefields of history’s first known cyber-war, the casualties are piling up. In the U.S., many banks have been hit, and the telecommunications industry seriously damaged, likely in retaliation for several major attacks on Iran. Washington and Tehran are ramping up their cyber-arsenals, built on a black-market digital arms bazaar, enmeshing such high-tech giants as Microsoft, Google, and Apple’.

It should be acknowledged that not all share this concern. For cyber warfare’s detractors, the coverage of cyber warfare illustrates typical media hyperbole, where popular dependence on technology - added to the mystique of exotically-named viruses and host of shadowy players - provides an irresistible combination for copy which simultaneously misrepresents and exaggerates the true nature of such action. Rid, questioning the designation of cyber operations as warfare, follows von Clausewitz’s dicta that an action needs to be violent, instrumental and political in order to qualify as war. Regarding violence, a true act of war requires actual or potential lethality.
Whilst the harm resulting from Malware could conceivably exceed the damage inflicted by conventional weapons, Rid reminds us that lethal effect has yet to be achieved in reality – the ‘casualties’ of the virtual battlefield remain virtual. For Rid, no cyber attack to date meets all three criteria of violence, instrumentality and political motivation, and only a few meet but one when subject to analysis. No incident to date has been publically attributed and acknowledged by a State, nor declared as an act of war, nor responded to with kinetic force. His conclusion is that cyber warfare is not warfare at all, but more accurately categorised as subversion, sabotage or espionage - activities which can support warfare but which do not stand as warfare in their own right.22

Security Lancaster acknowledges these reservations, but notes that despite its detractors, cyber warfare as a topic of credibility and importance in relation to both national and international security finds resonance with many countries at policy level, where it is gaining increasing momentum. We discern that the threat is taken seriously for a number of reasons which we list below as the 6 ‘A’ Factors of cyber warfare in Figure 1:

Figure 1: The 6 ‘A’ Factors of cyber warfare

- **All‐encompassing - the critical ubiquity of digital technology**
The pervasive and ubiquitous nature of digital technology has rendered technologically developed nations highly vulnerable to cyber attack, as much if not all critical infrastructure is in some way dependent on the internet. Moreover, as this critical infrastructure is increasingly privately owned, often by foreign companies, there is a need for countries to identify and defend their critical digital infrastructure as a matter of national security. Where the military are dependent on commercial infrastructures, the hostile targeting of those infrastructures may risk compromising civilians and other non‐military targets.

- **Acceleration – speed of attack**
Whereas in conventional warfare there may be a time delay between the declaration of hostilities and the start of military attacks due to the need to organise forces and overcome geographical distance, the instantaneous nature of cyber attack means that attacks can be launched immediately with instantaneous effect from geographically remote positions. Such acceleration lends heightened importance to defence considerations in particular. Acceleration may also refer to the exponential development of cyber weaponry in terms of its sophistication.
• **Asymmetric and Available – the entry of new players as belligerents**

The lower threshold of entry for cyber capabilities leads to pronounced asymmetries in warfare, and States with developed militaries are now facing threats from a potentially large range of new belligerents – not necessarily other States – who were previously unthreatening by virtue of their lack of conventional forces. Whereas the formation of conventional armament is controlled due to legal frameworks, budgets and manufacturing capacity/capability, the instruments of cyber warfare could be created much more easily, quickly, cheaply and surreptitiously as technology develops. Virtual groups spread over disparate geographical areas, driven by various ideological/religious motivations, can quickly form, attack, and disperse.

• **Amplification – the magnification of force though cyberspace**

Noting Metcalfe’s Law, the ubiquitous nature of networked infrastructure and related ‘Internet of things’ means that force is quickly and easily magnified though cyber operations, thus the potential scope of attack is larger than from conventional forces e.g. Malware could destroy the operation of a national power grid with far-reaching consequences.\(^{23}\) Whereas a conventional bomb might have a predictable blast radius, the ‘blast radius’ of Malware may be difficult to estimate.

• **Anonymous – the ability to plausibly deny attack**

Perhaps the most troubling quality of cyber operations from legal, military and political perspectives. Due to the nature of cyber warfare, attribution is very difficult in that unlike combatants, code does not bear identifying insignia and is more difficult to trace compared to conventional weaponry and attack. This quality permits belligerents to freely deploy cyber weaponry without having to take any responsibility or having responsibility attributed to them. The difficulty of attribution should not prevent States from considering attack seriously, especially as sophisticated attacks are likely to be State sponsored, likewise high deniability is precisely what renders cyber attack so threatening. Whilst features of Malware could tie sources of different attacks or weapons together, it is still difficult to trace source to identity.

2) The increasingly open acknowledgement of cyber warfare at International level

We note that an increasing number of military powers are considering their stance in relation to the threat, and policy documents are now emerging that articulate their positions in relation to cyber warfare. This is mirrored by growing political dialogue at international level. In 2010 the NATO Lisbon summit identified the cyber domain as an emergent security concern, a theme echoed domestically in the Strategic Defence and Security Review of the same year which designated online threats as a Tier One risk to national security.\(^{24}\) To place this in perspective, only three other Tier One risks were identified.\(^{25}\)

The Review initiated a comprehensive spending programme of £860 million, which included investment in developing military cyber capabilities. The London Conference of 2011, which brought together over 700 delegates from more than 60 countries, set cyber conflict firmly at the apex of the international agenda by setting it as one of five central topics of debate, an agenda sustained by London’s successor conferences of Budapest 2012, Seoul 2013 and prospectively the Netherlands 2015.\(^{26}\) Cyber conflict has also dominated diplomatic agendas at the highest levels, as noted most recently in relation to the 2013 Summit between the Premiers of the US and China following the Snowden revelations.\(^{27}\) Yet perhaps the most palpable (and poignant) acknowledgement of cyber warfare as a topic of political and military credibility is seen in its recent inclusion as a topic of importance for the International Committee of the Red Cross’s 2011 Report on International Humanitarian Law and the challenges of contemporary armed conflicts.\(^{28}\)

In order to give an overview of the tempo and trajectory of development in the field, **Figure 2** overleaf maps key developments in cyber incidents against developments in domestic policy, international conferences and significant publications, and International policy developments (see Appendix 1 for source data):
3) Legal uncertainty

It is notable that not all countries have a clearly declared stance on the military use of cyber operations, and whilst it is widely believed that China has an entire military section dedicated to cyber warfare, namely PLA Unit 61398, Chinese perspectives in particular are underrepresented in the debates.\textsuperscript{29} But where national stances are articulated, the significance given to cyber warfare can clearly be seen. The US strategy states that:

‘When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All States possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners. We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests. In so doing, we will exhaust all options before military force whenever we can; will carefully weigh the costs and risks of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support whenever possible’.\textsuperscript{30}
The UK strategy document observes:

‘Some of the most sophisticated threats to the UK in cyberspace come from other States which seek to conduct espionage with the aim of spying on or compromising our government, military, industrial and economic assets, as well as monitoring opponents of their own regimes. ‘Patriotic’ hackers can act upon States’ behalf, to spread disinformation, disrupt critical services or seek advantage during times of increased tension. In times of conflict, vulnerabilities in cyberspace could be exploited by an enemy to reduce our military’s technological advantage, or to reach past it to attack our critical infrastructure at home’.31

As indicated by the US Statement, precisely what States may do in reaction to a cyber attack or in pre-emption of such is a question that must be framed by law, but there may be several (and potentially intersecting) bodies of law that need to be considered. A difficulty is that potentially relevant laws have largely developed before the advent of cyber warfare and thus make no explicit reference to it in their key treaties and documents.

Cyber warfare in such policy documents largely comes under the broader heading of cyber security, which would include matters such as cyber-espionage, IP theft and the unauthorised manipulation of data. The phrase ‘cyber warfare’ is used in neither US nor UK policy document as it is not yet a term of legal art, and whilst the technology behind cyber warfare has moved apace, a complementary legal framework has yet to emerge.

If it is assumed that the silence on cyber warfare in the legal documents is not fatal and the law does indeed apply (there being growing opinion that it does) then the question becomes precisely how these laws apply as consensus needs to emerge as to how key terms are to be defined. Do new laws need to be drafted or can the existing ones be extended by analogy? The development of a legal lexicon associated with cyber warfare is thus more than an academic exercise as terms such as ‘attack’ have important existing legal as well as military meaning, and the addition of ‘cyber’ may strain the existing meanings.

Where to place cyber attacks in the existing legal framework – assuming it is fit for this purpose – is a difficult and arguably open question due to the emergent nature of the field, unique characteristics of cyber warfare and lack of authoritative and definitive legal statement on the matter. Precisely which legal paradigm/s ought to frame cyber warfare is itself a matter of considerable debate and also importance, as the designation may lead to significant differences in what legal rights and responsibilities flow. The section below notes the key bodies of law that may be relevant and then introduces the Tallinn Manual on cyber warfare, which is the most recent and authoritative attempt to outline how the relevant law might apply.

Potentially Relevant Bodies of Law: Public International Law (jus ad bellum, jus in bello/Law of Armed Conflict/International Humanitarian Law); International Criminal Law, Domestic Criminal Law and International Human Rights Law

If cyber warfare is to be understood in a legal sense, as being part of conflict between States, then it needs to be understood within the framework of Public International law.32 This body of law has arisen to promote harmonious relationships between States. The principal sources of law are treaties and custom, the latter being the law that has evolved from the practice of States. When determining disputes in International Law and advising on legal questions referred to it, the International Court of Justice may also consider judicial decisions and the teachings of the most highly qualified writers, but only as subsidiary to the main sources of treaty and custom.
The most fundamental rules of customary international law are known as ‘jus cogens’, compelling and overriding rules of law (an example would be the rule against genocide) which cannot be deviated from by States, even dissenting ones. States cannot ‘get round’ the rules of jus cogens by creating treaties to the contrary, as any treaties that conflict with a rule of jus cogens are considered void. An underlying principle of international law is that peaceful coexistence arises when States can exercise control over their territory in a sovereign manner, and challenges to this sovereignty are conceptualised along a sliding scale.

At the lowest end of the scale, it is recognised as a general principle that States are obliged not to intervene in the affairs of other States and to seek peaceful settlement to their disputes. Should States intervene in a forcible manner, then the action might be classified if sufficiently serious as a ‘use of force’, which is prohibited by Art 2(4) of the UN Charter. If an operation is found to fall short of a use of force, it may still be unlawful, in that it may be contrary to the principle of the non-intervention by States in each other’s affairs. ‘Use of force’ itself is not authoritatively defined in international law and the Charter gives no elaboration on how to determine when a hostile act amounts to a use of force but it may in part be defined negatively, so it is established that the use of force is not mere political or economic coercion. Nor does it include non-destructive psychological operations aimed at undermining confidence in an economy or a government.

The definition of use of force must depend on the circumstances and be determined considering the act’s scale and effects as noted in the Nicaragua judgment. If the scale and effects are sufficiently grave, then the use of force may be considered to reach the threshold of an ‘armed attack’, the most serious form of which is an act of ‘aggression’, the most censured and unjustified use of force, which due to its severity is categorised as a war crime. Aggression may incur personal liability for its instigators under International Criminal Law.

Although international law prohibits the aggressive threats or use of force by States, it is recognised the prohibition alone may not eliminate hostile gestures and acts entirely. The use of force in self-defence is thus permitted, but in limited circumstances. So as to avoid States taking matters into their own hands in times of dispute, the UN Security Council is mandated under Chapter VII of the UN Charter to determine acts of aggression, threats to or breaches of the peace, and to authorise appropriate measures - military or non-military - to address the situation.

However, this mandate does not extinguish the individual right of States to act in self-defence in the interim if necessary under Article 51 of the Charter. States may defend themselves – a right recognised as jus cogens – if they suffer an armed attack. Any defensive use of force must be conducted in a necessary and proportionate manner. Precisely when the right to self-defence may be invoked is a matter of contention, given the lack of clarity on judging when a use of force is sufficiently serious so as to amount to an armed attack, and also considering the lack of clarity regarding at what stage in time an anticipatory (and even pre-emptive) self-defensive use of force may be invoked, prior to an armed attack actually reaching the target State. States are the main initiators of armed attacks, but sufficiently grave uses of force carried out by organs of the State may also be categorised as such. Armed attacks are not limited to a State’s regular forces; non-State actors such as armed bands, irregulars, groups and mercenaries may also carry out armed attacks if they can be imputed to the State. Figure 3 overleaf summarises the spectrum of force/reaction in international law:
The law regarding the use of force described above is termed *jus ad bellum*, but a different set of rules in international law known as *jus in bello* may also be relevant. *Jus in bello* is also known as the Law of Armed Conflict (LOAC) or International Humanitarian Law (IHL). 35 Whereas *jus ad bellum* tries to temper the use of force, *jus in bello* recognises that if force is resorted to in certain circumstances, its worst effects must be alleviated. Thus rules are laid out to ensure that conflict is as humane as possible for all, whether civilian or combatant, so as to balance military necessity with humanity. 36

LOAC rules address matters such as the protection of civilians and medical personnel, rights for prisoners of war and the types of weapons that are permitted in conflict situations. The activation of *jus in bello* is not dependent upon the classification of the hostility under *jus ad bellum*, as *jus in bello* will apply even to an illegal (i.e. aggressive, unjustified) use of force under *jus ad bellum* if there is an armed conflict. The key to *jus in bello* is ‘armed conflict’ - an armed conflict is required for *jus in bello* to operate.

Armed conflict has traditionally been categorised as international (‘IAC’) or non-international (‘NIAC’) in character which has implications for the detailed rules that are applicable. The existence of an IAC triggers the full body of the LOAC, whereas NIAC triggers important but significantly more limited legal protections. 37

**International Armed Conflict**

An International Armed Conflict refers to hostilities between two or more States. As the armed conflict is between States (‘inter-national’), there is a trans-border element to hostilities. Arguably a threshold element of duration and intensity is required, so as to avoid the inclusion of mere border incursions and skirmishes. 38

**Non-International Armed Conflict**

NIAC is at least classically the legal label given to a civil war. The law applying to it was a subset of the wider law of armed conflict, but by the late 20th century it was the dominant form of conflict so the state of the law relating to it is increasingly important. NIAC is understood as referring to armed conflict that is conducted between a State and an organised non-State armed group, or between organised non-State armed groups, and geographically limited to the territory of a single State, however more recent arguments have suggested that an NIAC may ‘straddle’ more than one State. 39 Counterintuitive as it might seem, this is because if one party to the conflict is a State (e.g. the US), and the other is a non-state actor (e.g. Al Qaida) in another ostensibly friendly state (e.g. Pakistan), then it is arguable that the conflict is not ‘inter-national’ (i.e. between two States) and therefore if it rises to the threshold of armed conflict then it can only be a ‘non-international’ armed...
conflict, in legal terms. In NIAC, the parties involved must have a certain degree of organisation, and the violence must reach a certain level of intensity, which is a question to be determined with reference to the facts of each situation.

Although acts of terror as methods of warfare are considered war crimes and punished under international criminal law (the branch of international law that addresses atrocities of the severest nature, such as genocide), terrorism as a phenomenon is largely considered within the law enforcement paradigm (i.e. a matter for domestic criminal law) as it tends not to be understood as originating from State authority. Following the events of 9/11 the US announced a ‘global war on terror’. This ‘war on terror’ is not capable of overall characterisation, having manifested itself in legal terms variously as IAC, NIAC, and enforcement of criminal law – with a hotly contested set of boundaries between these characterisations, and profound implications for the relationship between them and, in particular, between the jus ad bellum and the jus in bello.

International Human Rights law (IHRL) may also be relevant, IHRL being the body of International law that is concerned with the protection of the individual against harms from the State. Commentators have observed that human rights considerations are increasingly being brought to bear on military situations. The complexity of conflict situations may lead to clashes between IHRL and LOAC because these bodies of law originate from fundamentally different standpoints. Whereas LOAC recognises that deaths may be a necessity in conflict, IHRL takes the standpoint that right to life is paramount and may only be derogated from under very strict conditions. In summary, Figure 4 below illustrates the main bodies of law discussed above and potential interplays between them.

Figure 4: Principal bodies of law and potential interplays between them

---

4) The Tallinn Manual on the International Law Applicable to Cyber Warfare

Consideration of how International Law applies to cyber warfare can be seen in the emergence of academic commentary on the subject which is, from around 2011 onwards, notably increasing in volume and frequency. However, this commentary has been largely un-coordinated. It is dispersed across a number of disciplines (security, computing, law, politics and international relations), is arguably sparse in relation to the importance
of the topic, and may potentially be narrow on the points that it considers. Some significant monographs and edited collections have recently been published, but again their number is not representative of the importance of the topic. Even relatively contemporary textbooks on international law do not mention cyber warfare, with indexes running straight from 'Customary Law' to 'Cyprus'.

In this respect, the publication of the Tallinn Manual on the International Law Applicable to Cyber Warfare 2013 has been a welcome intervention. Following a number of similar rulebooks on International law and warfare such as the San Remo Manual on International Law Applicable to Armed Conflicts at Sea and the Tallinn Manual on International Law Applicable to Air and Missile Warfare, the Tallinn Manual aims to provide a broad overview of international law rules applying to cyber warfare. It was compiled by an independent group of International experts, acting upon the request of the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) based in Tallinn.

The views expressed in the Tallinn Manual, though, are those of the experts themselves acting in their private capacity, and do not represent the views of NATO CCD COE, the sponsoring nations or NATO itself. As the Tallinn Manual itself notes, it is not a binding legal document, nor does it propose future law, best practice or preferred policy. Rather, it represents the views of the authors on what the currently applicable law is to cyber warfare. However, as the authors are eminent, it is possible that the Tallinn Manual’s views could represent subsidiary means for the determination of the rules of law for the International Court of Justice.

As the Tallinn Manual observes, there are no treaty provisions directly addressing cyber warfare and although International law may also derive from custom, it is difficult to establish (given the novelty of the field) whether there is always enough available material and practice to draw conclusions of customary law from. However, the Tallinn Manual starts from the position that the International Law of jus ad bellum and jus in bello do apply to cyber operations, and seeks to clarify the scope and manner. A number of observers participated in the discussions of the group of experts, including representatives from the United States Cyber Command, the International Committee of the Red Cross and NATO itself, but their consent was not necessary in determining whether a Rule was adopted in the Tallinn Manual.

Regarding scope, cyber criminality (understood as cyber activity that fell below the use of force according to the jus ad bellum understandings), was excluded from the scope of the Tallinn Manual as it was felt that these were best considered as a matter of domestic (criminal) law enforcement. Only where cyber activities were relevant to the law on use of force or armed attack were they considered. Whilst it was noted in the Tallinn Manual that matters such as cyber espionage and intellectual property theft may pose security risks per se, they were not risks that were seen to engage the international law rules on the use of force and armed attack.

Accordingly, the Tallinn Manual considered cyber-to-cyber operations in the strict sense, and did not consider traditional electronic warfare or kinetic-to-cyber operations, which both come under established legal frameworks. Commentaries accompanying the rules outlined in the Tallinn Manual illuminated any differences of opinion in the group of experts as to scope or interpretation, a spectrum considered particularly important by the experts given the immature nature of State practice and treaty application in the field. Treaties were cited when considering the rules proposed where available, and documents outlining customary law such as the ICRC Customary IHL Study were drawn on where possible in support. Military manuals from Canada, Germany, the UK and US were also consulted. In outlining the rules, the group of experts were unanimous in concluding that despite an absence of treaty provisions, the general principles of international law applied to cyberspace, as did the law of armed conflict. Arguably this approach does much to legitimise cyberspace as a viable space for conflict.

In applying the methods and medium of cyber warfare to international law, the Tallinn Manual considered the particular difficulties that cyber hostilities might engender. For example, when considering a threat or use of force, or armed attack, what thresholds would cyber operations have to reach to qualify as such? Would the scale and effects comparison work for cyber operations? Given the difficulties of distributed and anonymous networks, how would jurisdiction and State attribution work? Likewise, how would the laws of neutrality work regarding attacks routed through other States not involved in the conflict? Regarding non-State actors, how might these be accounted for in cyber hostilities, and how might armed conflict be conceptualised in LOAC terms in a cyber context?
The Tallinn Manual concluded that in certain circumstances, cyber operations could be considered on the international law spectrum of unlawful interventions, potentially rising to the use of force and even armed attack if sufficiently serious. Moreover, in the view of the experts, LOAC was applicable, as cyber hostilities could be conceptualised as armed conflicts, both in the context of IAC and NIAC, depending on a case by case analysis of each situation.
Section 2: Methodology and Structure of the Workshop

It can be seen from the outline above that there is considerable uncertainty in relation to cyber warfare. As summarised in Figure 5 below, the uncertainty can be seen to divide into three principal but related areas.

Figure 5: Political, conceptual and legal uncertainty

- **Political uncertainty**
  Whilst policy is clearly crystallising around cyber warfare, this is not happening uniformly. As noted above, not all countries have clearly articulated a stance and the underdeveloped policy position of China in particular is a matter of concern. If ‘rules of the road’ are to emerge that will apply to all, given that cyberspace is a global space, then a debate that reflects as many views as possible would be most desirable. Additionally, the war against terror as an instrument of national policy pursued by the US makes harmonisation potentially more difficult, as non-State actors are increasingly influential in the post 9/11 landscape, as seen for example in the Syrian Electronic Army. The fact that much national critical digital infrastructure is privately owned and/or maintained, often by foreign companies, further complicates matters in the creation of domestic security policy. What counts as the critical digital infrastructure in itself may be a matter of debate.46

- **Conceptual uncertainty**
  It has been noted above that there is contention as to whether cyber operations properly count as warfare in their own right, or whether they are better conceptualised as adjunctive methods of war that fall short of true force. The ‘warfare’ of cyber warfare certainly has multiple valences, and there is a question as to whether it is better understood as a metaphorical expression akin to the ‘war’ of the ‘war on obesity’ or in contrast as the art of cyber operations relating to conflict.

- **Legal uncertainty**
  If an act is not prohibited in International law, it is presumed to be permissible. In the absence of a specific treaty, there is uncertainty as to how the established customs of International Law apply, and how those rules might interface with other areas of potentially applicable law such as domestic criminal law and International Human Rights Law. Although as noted above there are an increasing number of State documents from which Statements on practice might be gleaned, it is questionable as to whether there is enough to suggest the emergence of customary law. Moreover, there is not necessarily any consensus as to whether the formulation of a new treaty would be desirable, or whether the law should emerge from the practice of States. If it does emerge from States’ practice, then the questions of which States and which practices get to be determinative are paramount. Whilst the publication of the Tallinn Manual is a welcome step, it is still an early intervention and by no means purporting to be the single, definitive view on the subject.
Workshop methodology and structure

It was at this stage - against a background of considerable uncertainty and a rapidly developing but fragmented field of expertise - that we decided to hold a Workshop on International Law and Cyber Warfare. The publication of the Tallinn Manual as the first coherent and systematic 'legal' intervention in the debate in particular invited response, debate and evaluation. We wanted horizon-mapping discussions that would enable us to create a timely research agenda that was relevant to key stakeholders in the debate, so we decided against holding a purely academic conference which we feared would give too narrow a perspective.

We felt that a Workshop format would facilitate the widest set of responses and viewpoints, and this also ensured that there was engagement with key external stakeholders. We wanted a blend of participants from defence and academia so that we could explore mutually relevant questions so as to map out future directions for relevant research. Following the format of previous Security Lancaster Workshops we planned to have a small round-table discussion. From the academic side, we were particularly keen to have an interdisciplinary range of views around the table. Academics were co-ordinated by Dr Bela Chatterjee, who invited two colleagues with expertise in international law and conflict – Dr Jackson Maogoto from Manchester Law School and Dr James Summers of Lancaster Law School – and Dr Mark Lacy from the Department of Politics, Philosophy and Religion at Lancaster, invited for his expertise in geopolitics, security, digital technology and war. Attendees from a wide range of Ministry of Defence establishments were co-ordinated by Lt. Cdr. Adrian ‘Tel’ Venables RNR, who also secured the Defence School of Policing and Guarding, Southwick as the Workshop’s venue. Dr Daniel Prince, the Security Futures project co-ordinator, acted as a consultant for the project, advising at the planning and report stage.

Bearing in mind the nature of the project, discussions were held at an Unclassified level. In order to ensure a free flow of discussion and ideas we considered the Chatham House Rule. The rule States as follows: ‘When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.’ The Chatham House Rule allows people to express their ideas at such meetings as individuals. Lists of attendees are not publically circulated and records of meetings after the event are described so as not to publically attribute, either implicitly or explicitly, specific viewpoints or comments to specific individuals. Given that the event was a mixed academic and MoD event, and with a view to the publication of the research report, it was decided that a modified version of the Chatham House Rule would be adopted, that is to say that it would cover the MoD attendees whilst allowing the identification of academics attending the event without attributing viewpoints to any particular one of them (or indeed any other attendee).

Our Workshop took place over the course of a day, and was semi-structured so as to provide some broad guidance without restricting the debate. So as to seed the ground, we put forth some initial questions which were largely prompted by the publication of the Tallinn Manual and framed by its scope as a document concerning international law as opposed to domestic criminal law and international human rights law:

- Was the Tallinn Manual sufficiently comprehensive from a military and legal perspective in its coverage of cyber warfare to contribute to the planning and conduct of military operations?
- Did the Tallinn Manual go far enough in its guidance and if it fell short, where could it be developed?
- What alternative positions might be taken that had not been envisaged by the Tallinn Manual?

Given the prominence of the Tallinn Manual as the first systematic and comprehensive attempt to map the relevant international law in the area, we had initially envisaged that discussion would be closely centred on it. However, the resulting discussion, enriched by the different fields of expertise around the table, led us to different points of inquiry not anticipated by our opening set of questions. In fact, our initial questions were quickly abandoned, as whilst the Tallinn Manual provided a touchstone for debate, it soon emerged that the matters of interest were at the margins of the Tallinn Manual’s scope - related to, but not falling squarely within, the frame of international law. This was helpful in causing us to critically reflect on our approaches to the field and reconsider whether isolating the discussion of cyber warfare discretely within an international law frame was the best approach to take.
Section 3: Proceedings of the Workshop

We outline the summary of discussions below, organised around key points of interest. Initially, some detailed exposition of the Tallinn Manual’s position on various points [in italics] is included of necessity, in order to frame our discussion and indicate our points of development and departure.

What counts as use of force?

The Tallinn Manual was drafted with more serious deployments of cyber operations in mind, i.e. reaching the use of force and armed attack, as these were the existing and relevant thresholds in international law. Accordingly, the Tallinn Manual extensively discusses both concepts. Whilst illegal threat or use of force was undefined in international law, following the existing position on political and economic pressure, the Tallinn Manual took a view that use of force in the context of cyber operations excluded political or economic pressure per se as well as non-destructive psychological operations and propaganda. Cyber espionage and the theft of IP would also not be considered as illegal uses of force, and were considered to be part of criminal law enforcement paradigm.

Where cyber operations injured or killed people, or damaged/destroyed property, the Tallinn Manual considered that these would be uses of force, echoing the kinetic definitions of use of force. Whether cyber operations that fell short of such impact counted as uses of force depended in the Tallinn Manual’s view on a consideration of their scale and effects. Factors that might help States assess the scale and effects could include the severity of effects, which could be considered in relation to the extent that operations impinged on critical national interests, and the scope, duration and intensity. Immediacy of effects could be considered, as could the proximity between actions and their effects. The degree of invasiveness could be considered, as could the measurability of effects, military character and extent of State involvement.

What counts as armed attack?

A similar approach was taken by the Tallinn Manual in defining armed attack for the purposes of cyber warfare. An armed attack could include cyber attack where the scale and effects were sufficiently grave, scale and effects to be evaluated on a case by case basis. Cyber attacks causing personal injury/death and/or damage/destruction of property would certainly count in the view of the drafting experts, whereas cyber intelligence gathering, cyber theft or cyber operations that caused sporadic or temporary disruption to non-essential cyber services would not qualify. There was disagreement amongst the Tallinn experts as to whether a cyber attack on a major stock exchange would be an armed attack. All armed attacks would be uses of force, but as the Tallinn Manual notes, there is a lack of international consensus as to whether all uses of force would count as armed attacks.

Who carries out armed attacks?

International law traditionally holds that States carry out armed attacks. Non-State actors may also carry out armed attacks if those acts are attributable to the State, for example groups acting under State direction. However, in the absence of direction by a State, attacks by non-State actors have traditionally been considered as terrorist actions, falling within the law enforcement paradigm and not initiating the right to self-defensive use of force. As noted by the Tallinn Manual, the State practice of the US in reaction to attacks by Al Qaeda has complicated this position in that the response has been articulated as a global ‘war on terror’, and self-defence has been invoked as a rightful response.
The Tallinn Manual’s focus on international law and the use of force paradigm led us to some interesting developments and points of departure. We considered in particular a number of interlinked themes:

- **Reconceptualising use of force and armed attack in the context of new belligerents and new methods of belligerency**
- **Reconceptualising States as prime movers**
- **Challenging the adequacy of international law as the prime conceptual framework in cyber warfare**

Whereas the Tallinn Manual was drafted primarily as a practical tool for professionals such as military and foreign office lawyers, we discussed how it concentrated largely on the more extreme end of the spectrum i.e. use of force and armed conflict. The Tallinn Manual largely addressed the threshold question of whether international law applied, but now that consensus was mounting that it did, the question turned to how it applied, particularly in relation to less extreme operations. We noted that broad coverage of cyber ‘attacks’ in the media was descriptive of the more widespread and quotidian phenomenon of lower level hostilities that fell short of use of force and armed conflict. Advice for the private sector was felt to be particularly useful in this context, given the proportionately larger number of actors here as opposed to in other domains.

For States and private sector actors facing hostile operations, there was discussion as to how international law other than that of *jus ad bellum/jus in bello* might structure a government’s advice as to how to respond. Some of us wished to consider how international economic law, for example, might be considered in framing the response to lower level hostilities such as initial probes into systems and commercial cyber espionage, and whether international legal structures such as the WTO might play an increased role in such contexts. It was possible that the emerging State practice on such matters might influence some of the positions articulated in the Tallinn Manual itself. Other delegates also questioned, however, whether the designation of some cyber operations as strictly criminal and thus domestic matters was a desirable stance. Whilst some of our discussants noted that the Budapest Convention on Cybercrime provided a framework for co-ordinating international responses to criminal matters, others observed that the potential linkages between the State and the criminal fraternity challenged the desirability of such strict legal demarcation. Attribution to a State itself remained a problematic issue.

Regarding criminal actions, we noted that increasingly that there were potentially concrete linkages between States and the criminal fraternity. We noted how patriotic hackers may be unofficially encouraged or supported by States. It was also observed that military hostility could come from freedom fighters and secessionist movements funded or supported by the criminal fraternity. The criminal fraternity could be considered as the ‘laboratory’ for new hostile cyber activity; activity that may well be supportive and used in furtherance of an irresponsible State’s interests. The theft of IP as State-sponsored could conceivably be a criminal act that supported the irresponsible State’s interests at the expense of the victim State, for example a scenario where software developed by a private company for the military market was the target of IP theft. Thus, some felt that there was a danger in conceptualising State actions and criminal actions as strictly separate phenomena. Additionally, considering a matter as falling within the ambit of States’ individual domestic law risked an uneven approach.

Given the centrality of the financial markets to national interests, we too questioned whether cyber attacks on financial institutions should be excluded from the use of force/armed attack paradigm. Disruptions in banking services affected the citizenry as a whole and raised the question of whether financial networks and institutions could or should be considered as critical digital infrastructure. Such an attack would engage the essential interests of the State, and the political response could shape whether an attack would be seen to rise to an armed attack. Cyber operations causing indirect effects on the banking sector could also be considered. For example, the actions of the Syrian Electronic Army in hacking Twitter feeds to spread false rumours about a bombing in the White House led to downturns in the stock markets. The interconnected nature of the internet made it difficult to determine a precise geographic locus of attack, such that DDoS ‘tennis matches’ between different factions could feasibly affect a wide number of users in different locations. Given the increasing dependence on cyber infrastructure, an electronic blockade could be feasibly be a serious action that could be conceptualised as forceful. However, some of us considered that whereas a cyber attack on the stock exchange might well invite a response, it might be questioned as to whether that response would be one of kinetic force in the current political climate.
The discussions on cyber attacks affecting stock markets led us to question whether the threshold of response, considered in terms of equivalence to kinetic effects, left us vulnerable. This was a slightly different problem to that of pinprick attacks, where the cumulative effect of small attacks added up to a larger whole. Rather, the issue was the danger of a hardening ‘lack of response’ norm which in turn could engender increasingly audacious operations in the face of apparent acquiescence. Particularly given the constant reports of cyber operations against companies and government institutions in the media, where suggested responses appear to be ‘defend better’ in a passive manner as opposed to utilising a more active range of responses permitted by law, there was a question as to whether a ‘stiff upper lip’ stance would send a negative message that such operations would be tolerated, leading not only to the threshold of response being set too high initially, but being subsequently raised each time an operation was unanswered. Some of us questioned whether the delegation of such a serious issue of national security was appropriately placed in the law enforcement paradigm.

We further considered that increasingly, adversaries were less likely to be other States. Interest groups in cyberspace could be highly fragmented. Hostile actors could be federated or balkanised networks that lacked any clear State affiliation. Yet international law was centred on the notion of sovereign States. As the nature of the adversary was changing, a legal framework that primarily concentrated on State to State actions could potentially be a hindrance.

Our discussions thus led us towards a critique of the current legal frameworks. Some of us were of the view that the current frameworks were unproblematic, particularly as international law was a flexible body of law: its lack of precise definitions gave a lot of scope in interpretation to grey situations, scope that could profitably be brought to bear on evolving situations such as cyber warfare. However, others felt that the existing legal approach was beset by binary thinking (e.g. a matter is either international or domestic, State actor or non-State actor) that failed to reflect the subtle and potentially plural linkages that arise from cyber hostilities. By imposing current legal thinking on the emerging phenomenon of cyber hostilities, there was a danger that cyber hostilities would prove ill-fitting, and that lack of alignment could be exploited by enemies. There was an understanding that the geometry of contemporary conflict tended not to be described by an equal meeting of State belligerents, but rather non-State actors, federated or balkanised networks, and this complexity needed to be recognised and reflected in law. This led us to consider whether States should have a broader spectrum of legal frameworks to consider, or whether a more singular but holistic framework was desirable.

Developing this line of thought, we considered whether in fact cyber conflict prompted a more radical break with international law, such a departure already being pre-empted by the ‘war on terror’ in the post 9/11 landscape. The template of reaction to Al Qaeda (considering as potential NIAC) might usefully considered as a way of theorising actions against diasporas of co-ordinated hacker groups driven by a common ideology. If legitimate use of force against Al Qaeda has been taken, then could use of force against such hacker groups be seen as analogous? It was noted that international law was an historic phenomenon that had been accreted over time and was grounded in historic concepts of State sovereignty and geographic territorial boundaries. However, as observed above, the nature of warfare and opponents had changed, and thus it was increasingly the network and not the nation that we were dealing with. The focus was then less on States, and more on networks and the nodes within them, networks themselves being increasingly federated, fragmented and/or balkanised.

If this was indeed the military situation that was increasingly being faced, some of us questioned whether any legal framework that attempted to address it would be better starting with the network itself, as opposed to the nation State. The difficulty of attributing responsibility to a State also rendered State responsibility as the central mechanism of analysis and action less helpful. The concept of sovereignty itself required rethinking using a networked approach, in a way which would describe and reflect the contemporary dynamics of power/influence of cyber belligerents as opposed to legal categorisations of actors based on historical constructs. Such an approach might capture the asymmetrical dynamics that were considered to be characteristic of cyber belligerents. Accordingly, a networked approach might thus be closer to reflecting the military reality on the ground. The concept of neutrality could also be challenged in the context of a network that was owned, especially where the effects of the actions of individual nodes in that network were felt remotely elsewhere.
• **Considering the definition of armed attack and threat of force**

Considering potential hostilities from federated or balkanised networks, we questioned the difficulties of conceptualising armed attack within the context of cyber warfare, particularly in relation to NIAC. We discussed the difficulty of determining a threshold of violence in cyber attacks, and raised questions regarding the degree of organisation that might be required. We also discussed the difficulties in maintaining a constant duty of care in cyber conflict, and questioned whether more co-ordination of international law might be required here.

Given that many cyber attacks could dwell comfortably below the threshold of use of force, threats of force were another difficult issue that we discussed. We questioned what the appropriate threshold would be for a threat of force to manifest. For example would the bare placement of Malware that was capable of later activation count as a threat of force? Would a mere probe into a system constitute a threat of force? It was noted that emerging belligerents could potentially have more advanced cyber capabilities than more established States, as they were not weighed down by legacy infrastructure. This insight led some of us to observe that there was a further difficulty in how the credibility of a threat was to be ascertained, and whether the cyber operation itself was the threat.

The discussion of threats linked in with a consideration of the problems of urgent countermeasures and anticipatory self-defence. It was questioned where countermeasures lay on the spectrum of active and passive defences, the latter themselves categories open to considerable interpretation. There were questions as to whether urgent countermeasures could be taken against non-State actors, and what this implied for belligerents who were federated/balkanised networks. Regarding anticipatory self-defence, there was a question as to how to calculate the immediacy of the situation. For example, at what point does a probe become an attack for the purposes of anticipatory self-defence – does this point come before or after the payload is executed? We considered that threat monitoring may well be the way to anticipate such situations, and judgements could be context-based.

We noted that it could be more than a decade or so until we faced belligerents with full cyber capabilities, and that we were currently in a ‘honeymoon’ period where adversaries were mainly heavily funded and sophisticated, but ultimately ‘small fry’. What preparations might be taken in anticipation for the ripening of cyber capabilities were not necessarily best concentrated solely in the cyber domain itself – we noted, for example, how some governments were seen to be investing in more traditional technology such as typewriters to ensure a substratum of operating infrastructure in the face of cyber attack.

• **Cyber operations as a ‘peacekeeping’ mechanism?**

As noted above, there was a view amongst our delegates that most cyber attacks would fall below the legal thresholds of armed attack and use of force. However, as noted above the International legal framework considered by the Tallinn Manual does not concentrate on cyber operations that fall below these thresholds. **Our discussions on lower-level cyber operations thus led us to considerations of conflict avoidance, where cyber operations could be seen as a preventative measure.**

We envisaged a circumstance where a weak or unstable State was in a pre-war, phase zero situation but clearly ripe for dangerous escalation. Such instability, if allowed to escalate, could pose a danger to remote as well as neighbouring States. In such a scenario, it may be difficult to identify who key actors are, and cyber operations might be needed at a broad social level. **Considering the non-intervention principle of International law, some of us questioned what cyber operations that fell below the use of force might be lawfully engaged in so as to stabilise the situation, for example by manipulating NSM feeds to influence social understanding.** Would such interference rise to the level of intervention? Would interference equate to intervention? What intervention might mean in the cyber context was worthy of consideration, for example would breaking into the fibre-optic cables to degrade/interrupt the service count? In this respect, intervention could valuably be considered from the wider perspective of customary law, where broader conceptualisations of intervention could come into play in the cyber operations context.

• **Practical Implications of cyber warfare for combatants on the ground**

Whilst the frame of international law tends to focus on State actors, our attention was also focused on the practical implications of cyber warfare for the combatant on the ground. It was observed that warfare was in
a transitional state in several respects which had relevance for the potential liabilities of the individual. Accordingly, we needed to look beyond the framework of international law to get a fuller picture.

It was observed that warfare was now moving increasingly towards the digital. Technology is now a pervasive aspect of military operations. The conduct of operations is now commonly carried out in a 24-hour media zone and the arena of combat itself is increasingly digitised. As contemporary warfare moves to cyber warfare, cyber defence may engender new norms of political coalition between allied States. Information streams and software platforms for imagery and virtual representations of the geographical battlefield and potential targets therein may come from coalition partner States and/or private suppliers. Much personal data may also be carried on smart ID cards.

The framework for decisions as to legitimate targets is dictated by the LOAC, but the military may be reliant on whichever products they are provided with in the conflict zone. If decisions to prosecute specific targets are made in reliance on data such as described above, questions arise as to the integrity of the software, and the point at which the human intuition of the combatant on the ground may be exercised. Questions of integrity arise on a number of grounds. Private/commercial (and potentially coalition partner) software may have questionable security; questions arise as to the reliability and validity of the information presented to the combatant on the screen. As data may be carried in motion across multiple networks not necessarily within the State’s control, what assurance does the combatant on the ground have that the information stream relied on has not been hacked and corrupted by the enemy?

The fine decisions that need to be made in reliance on technology are linked to questions about the personal liabilities of combatants. Traditionally, individuals aggrieved in warfare may seek justice through their own State, whereby the State initiates legal action against an international person on behalf of the claimant. Whereas this mechanism is a State-to-State one where matters remain on an international level, it was observed that increasingly, conflict may engender civilian claims based on human rights grounds that are brought against individual combatants. This is particularly so where multiple State forces are in coalition and/or orchestrated by an international organisation such as NATO, as States may be unwilling or unable to bring claims on behalf of their citizens.

For individual combatants, the possibility of personal civil liability may be of great concern, especially if individual decisions on targeting are based on software and information streams that are not within their control. Anxieties may be magnified if the limitation period for such claims is uncertain, as individual combatants could be questioned regarding decisions made a long time after the combat has ended. The transition of traditional warfare to cyber warfare may itself make the distinction between the start and end of conflict difficult to discern.

Regarding smart ID cards, we considered the scenario where such cards might be lost in a conflict zone, and obtained by the enemy. The enemy could use the personal information on the cards as a basis for targeting connected individuals in the home combatant’s country. We questioned whether duties of care might arise for the State in relation to those individuals whose information had been compromised, for example whether there was a duty to warn.

Specific questions thus arose as to the nature and scope of individual liability for actions taken in cyber combat, and whether the framework of international law was the best starting point for consideration in this respect. A critique of individual liability was needed in the context of International Human Rights law and potentially International Criminal Law, and consideration of how increased liability under Human Rights law in particular might affect military actions and reactions in the field. The potential liabilities and duties of care of private suppliers of software also needed consideration within this framework, as did the responsibilities of commercial service providers such as ISPs – a question of broader relevance to cyber warfare as a whole, considering the increasingly privatised nature of global communications/infrastructure systems. This question would be of increasing importance as sophisticated software to be used in command and control might soon be produced by commercial partners.
• **Related software questions - collateral damage, escaped software, digital decontamination and duties of care**

The discussion on the validity and reliability of software in combat situations led us to consider liabilities regarding the practical deployment of cyber weapons of integrity as opposed to those compromised as discussed above. This led us to consider a number of issues relating to collateral damage, the liabilities for escaped software and the question of whether ought to be a duty of digital decontamination in the aftermath of a digital attack.

LOAC is underpinned by the principle of distinction. This holds that only military objectives may be legitimately pursued so as to restrict the effects of war as far as possible. Civilian populations and combatants must be distinguished, as must civilians, civilian objects and military objectives; only military objectives can be pursued. Proportionality is also key; attacks may not be excessive.

Cyber warfare raises interesting questions regarding how the principle of distinction and proportionality apply to digital weapons and environments. These are noted by the Tallinn Manual, which considers the difficulties posed by cyber communications networks used by both civilians and the military. It is established law that an object can either be military or civilian, but not both simultaneously. Military use renders a dual use network a military object, even if it continues to have civilian uses. The Tallinn Manual suggests that a cyber attack that indiscriminately targets and damages a dual use infrastructure where it is possible to direct the attack at specific military objectives within is prohibited, in that the attack could have been narrower. It also notes that cyber attacks must be proportionate, in that they must not cause loss or injury to civilians or civilian objects that are excessive in relation to the military advantage anticipated.

It is possible that Stuxnet-type Malware may be distributed across the civilian network with the aim of finding its way to a military objective, and the Tallinn Manual considers the legality of such an attack in terms of discrimination and proportionality. This led us to consider the question of digital collateral and how it might be calculated as it is difficult to ‘count the bodies’ in cyber warfare as damage may be non-tangible. Software in a cyber attack may be designed to accord with the principle of distinction and intended to be proportionate, but it may be difficult to envisage what proportionality might look like in the cyber theatre of operations, particularly in the context of dual-use networks and the move towards an ‘internet of things’.

Accordingly, the expected degree of collateral damage - including damage in transit over a communications system as well as that resulting from the attack itself - might be difficult to ascertain. **We observed that damage may not be immediately apparent, thus the timeframe for estimating damage is uncertain, and the potential nature and scope of damage may be difficult to predict and estimate, especially with software at the cutting edge of development.**

The theme of collateral damage further invited us to consider the nature and scope of duties of care in relation to ‘escaped’ software and the question of digital decontamination. It was recalled that software supplied may not originate from the military, and thus questions were raised as to the scope and nature of any duties of care. Ought there to be such duties, and if so who might owe them - would they adhere to private suppliers or other non-State organisations? **As damage to networks might be extensive, the question arose as to whether there should be a duty of digital decontamination and what the scope of that duty might be.**
Section 4: Conclusions

An Agenda for Future Research

What did we learn from the Workshop? Our conclusions can be divided into macro- and micro-level insights:

- **At a macro level:**
  We learned that State-on-State cyber war was less of a concern than we had initially envisaged; most if not all cyber attacks were anticipated to be at a sub-warfare threshold, thus there was a greater concern with the legal framework (both international and domestic and the interplay between them) relating to such actions. It was felt that the high political stakes made open State-initiated cyber warfare unlikely, especially in a pure form. Cyber warfare was seen to be but one weapon in the box of conventional arsenal, as opposed to a modality of warfare that would eclipse all others.

  We also learned that the identification of States themselves as prime actors was itself problematic in that cyber capabilities created asymmetric warfare; whilst international law tended to conceive of principal actors in terms of equal States, belligerents may no longer be States but private actors, federated or balkanised networks that transcend State boundaries and have no distinct State affiliation.

  We noted that the legal categorisation of incidents could be problematic and a focus on international law in isolation inadequate, in that the identification of incidents as either domestic criminal or international law matters was not felt by all to adequately reflect the potential links between criminals and States when the proceeds of crime could further State activities and interests. Especially given the problems of attributing cyber actions to States, the role of non-State actors in cyberspace certainly needed greater consideration, either as commercial providers of infrastructure and software or as ideologically motivated activists.

  Due to the emergent nature of the field and also because of a lack of consensus, it was felt that there was some lack of precision and clarity with key terminology. The lexicon of the emerging field needed careful thought – we noted for example that seemingly common terminology such as ‘attack’ lacked uniformity and consistency of meaning, for example media reports of cyber ‘attacks’ may not coincide with the legal/military understanding of the term. The definition of attack specifically within the law of armed conflict required thought in the context of cyber operations, particularly the nexus with violence and whether purely cyber operations could indeed be categorised as violent.

  Interestingly, we discovered that warfare itself might not be the most fruitful question to focus on: there was interest in how cyber capabilities, for example the manipulation of social media networks, could be used to influence weak or unstable States in a pre-warfare position so that the situation did not escalate – the legal framework relating to cyber ‘peacekeeping’ and the legality of cyber intervention by a stronger/more stable State to further this aim being an intriguing reversal of the initial question of cyber warfare.

- **At a micro level:**
  There was particular interest in the practical implications of cyber warfare for the combatant on the ground, particularly connected to private actors as software/critical infrastructure suppliers. Points of tension arising did not always relate discretely to international law. For example, the increasing use of software to identify and prosecute targets led to questions of the integrity of that software. If provided by non-military suppliers, how would combatants know whether information streams were sound or corrupted by enemy hacking, and what personal or other liabilities might flow from decisions taken in reliance on it, particularly as affected individuals look increasingly to Human Rights jurisprudence as an effective mechanism of redress?
Further, related questions emerged:

- If digital weapons were used what might collateral damage look like?
- What were the liabilities regarding ‘escaped’ software, and was there a ‘duty of digital decontamination’ to reconstruct damaged systems?
- More broadly, what is the scope of duty of care in cyber operations and by whom is it owed – does this include non-State actors?

**Methodological insights:**

The pattern of discussion led us also to some methodological insights, which were as important as the identification of discrete areas of focus for future research. We concluded that a methodology that questioned the traditional boundaries or categorisations of legal analysis could be beneficial – a more holistic approach was needed if our future research was to reflect the complex reality of cyber operations. The approach to future legal research would need to be less ‘compartmentalised’, and the delineation of problems into exclusive legal categories would not necessarily be helpful or accurate.

*In sum, the above discussions lead us to draw out four underlying principles that can be applied to the area, and six discrete areas of interest that can be expanded on to produce an informed research agenda. The principles and areas of development are as follows:*

**Underlying Principles**

1. The concept of war as symmetrical State-on-State conflict needs challenging. Although the Tallinn Manual considers international law and thus focuses primarily (although not exclusively) on States, we suggest that the principal belligerents in cyber warfare are unlikely to be States themselves, and the role of non-State actors in particular is unlikely to be adequately addressed by a focus on international law and the use of force paradigm alone.

2. Linked with principle 1, a more holistic approach to legal research is needed if research on cyber warfare is to reflect the complex reality of cyber operations. In particular the interplay between international and domestic law needs to be more extensively considered to reflect the hazy boundaries between States, non-State actors and the criminal fraternity.

3. A focus on cyber peace might be as productive as a focus on cyber war – a promising channel of investigation opens up regarding the role of cyber intervention in weak/unstable States and the legality of such intervention.

4. The lexicon of cyber warfare needs careful thought, and key terminology needs to be defined and considered in its particular context. Multiple valences need to be articulated as clearly as possible if interdisciplinary/contextual work is to be conducted.
Six areas for development:

- What is/should be the legal approach to cyber warfare conducted by non-State actors and/or federated/balkanised networks, and what liabilities and obligations might lie with non-State actors more widely in relation to cyber weaponry and critical digital infrastructure?
- How should the ‘attack’ of cyber offensives be conceptualised within the Law of Armed Conflict? Should the conceptual framework of kinetic attack be extended by analogy?
- What legal questions emerge from the manipulation of social media networks etc. to de-escalate situations of tension in weak/unstable States?
- What personal or other liabilities might flow from combatants’ reliance on information streams produced by software provided by private suppliers/coalition partners?
- Is there a duty of ‘digital decontamination and reconstruction’ regarding cyber operations?
- What is the scope of the duty of care regarding cyber operations and by whom is it owed?

Did we achieve our aims?

A central aim of Security Lancaster is to facilitate the exchange of ideas and information through the sharing of facilities, the creation of networks of like-minded individuals, and through the development of a ‘social infrastructure’. Another is to deliver world leading research in security sciences by balancing basic research with use-inspired and applied research to ensure that the output remains both theoretically rich and relevant to societal needs and priorities. We conclude that the Workshop saw Security Lancaster successfully furthering these aims by creating a coalition of key stakeholders so as to raise awareness, identify and explore relevant security/legal questions relating to cyber warfare. This led to the creation of an informed research agenda which can be developed and addressed by engagement in more detailed pieces following on from this report.
Section 5

Key Legal documents and cases

Helsinki Accords/Helsinki Final Act 1975
Rome Statute of the ICC 1998
United Nations Charter 1945
United Nations General Assembly Resolution 2625 (Declaration on principles of international law concerning friendly relations and cooperation among states in accordance with the Charter of the United Nations) 1970
United Nations General Assembly Resolution 3314 (Definition of Aggression) 1974

Nicaragua v USA 1986 ICJ Rep 14
Smith v The Ministry of Defence [2013] UKSC 41

Glossary

Armed attack – In international law, a sufficiently grave use of force which qualifies by virtue of its scale and effects as an armed attack. Scale and effects are defined by circumstance. An armed attack triggers the victim State’s right to proportionate self-defensive use of force in international law. An armed attack is graver than a use of force, so whilst an armed attack will be at least a use of force, not every use of force will amount to an armed attack.

International Armed conflict (IAC) – In international law, IACs refer to hostilities arising between two or more States. As the armed conflict is between States (‘inter-national’), there is a trans-border element to hostilities. Arguably a threshold element of duration and intensity is required, so as to avoid the inclusion of mere border incursions and skirmishes. As noted by the Tallinn Manual, the term ‘armed conflict’ has never been authoritatively defined as a matter of treaty law. It has come to replace ‘war’ for the purposes of the law of armed conflict.

Non-International Armed conflict (NIAC) – In international law, NIAC is at least classically the legal label given to a civil war. NIAC is understood as referring to armed conflict that is conducted between a State and an organised non-State armed group, or between organised non-State armed groups, and geographically limited to the territory of a single State, however more recent arguments have suggested that an NIAC may ‘straddle’ more than one State. In NIAC, the parties involved must have a certain degree of organisation, and the violence must reach a certain level of intensity, which is a question to be determined with reference to the facts of each situation.

Customary international law – international law that has developed and emerged from the practice of States.

Cyber operations – A generic term undefined in law that can broadly be understood to mean the use of cyber capabilities directed at specific objectives, which may or may not amount to cyber warfare depending on the context.

Cyber warfare – A generic term undefined in law which for the purposes of this report refers to those cyber operations which engage international law and use of force paradigms. This report also suggests a critical approach to this definition in questioning whether cyber warfare ought to be dictated exclusively by such paradigms.

D/DoS – Denial of Service attack – the denial of service to the actual/potential computer user, Distributed Denial of Service attack as above, involving two or more computers, such disruption usually being the result of a cyber operation.

Flame – A sophisticated and sizeable espionage-style Malware that has been infecting systems in the Middle East and North Africa; widely believed to be State originated.
ICC – International Criminal Court.
ICRC – International Committee of the Red Cross.
Internet of Things – a phenomenon whereby everyday objects are capable of connecting to the internet and transmit/receive data through RFID tags and chips or similar.
International Criminal Law – branch of international law addressing the gravest of crimes such as genocide.
International Economic Law – branch of international law addressing the conduct of States in their international economic relations.
International Humanitarian Law – see LOAC.
International Law – law which regulates the relationships between States.
Jus ad bellum – international law addressing the legally acceptable use of force.
Jus cogens – fundamental rules of customary international law that cannot be altered by treaty
Jus in bello – see LOAC.
Law of Armed Conflict (LOAC) – branch of international law addressing how armed conflict is conducted. LOAC aims to ensure that armed conflict is conducted as humanely as possible for all concerned, whether civilian or combatant, once it arises.
Malware – software implemented for the purpose of disrupting the correct operation of computer and network-based systems.
Moonlight Maze – An incident where American officials discovered unauthorised computer system probes focused on organisations such as NASA, the Pentagon and the Department of Energy.
Non-intervention – a principle of international law whereby states refrain from interfering in the sovereign affairs of other states.
NSM – New Social Media.
Operation Aurora – A coordinated attack including a piece of computer code that exploits the Microsoft Internet Explorer vulnerability to gain access to computer systems. This exploit is then extended to download and activate Malware within the systems – see http://www.mcafee.com/us/threat-center/operation-aurora.aspx
Shady RAT – Operational name given to a series of cyber attacks on various global actors and organisations (RAT = Remote Access Tool)
Stuxnet – Highly complex Malware discovered in 2010 which was reported as having the effect of sabotaging Iranian nuclear centrifuges and widely considered to be State originated.
Titan Rain – name conferred by the US on a series of malicious co-ordinated attacks on US computer systems.
UN Charter – foundational treaty of the UN which outlines (amongst other things) rules promoting the harmonious co-existence between States.
Use of force – a term of international law not authoritatively defined but understood to infer a degree of hostility and excluding pressure of a political, psychological or economic character. An act which is found to fall short of a use of force may still be prohibited under international law as being against the principle of non-intervention.
WTO – World Trade Organisation.
Documents and sources are listed alphabetically by title or institution/organisation where no author is apparent


*International Law Studies* (2013) 89 (special issue on international law and cyber conflict)


http://www.lancaster.ac.uk/news/blogs/mark-lacy/the-syrian-electronic-army-is-rewriting-the-rules-of-war-


Lindsay, J. (2013) ‘Stuxnet and the Limits of Cyber Warfare’ Security Studies 22 (3) 365-404


London Conference on Cyberspace (2011)
http://www.chathamhouse.org/research/security/current-projects/london-conference-cyberspace (archive site);


MoD Defence Cyber Operations Group Cyber & Influence STC CDE Call Launch (MoD Slide Show 2011) www.science.mod.uk/controls/getpdf.pdf?606


Netherlands Conference on Cyberspace 2015


http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0

Schactman, N. (2013) ‘This Pentagon Project Makes Cyberwarfare As Easy As Angry Birds’
http://www.wired.com/2013/05/pentagon-cyberwar-angry-birds/4


Securing Britain in an age of uncertainty: The Strategic Defence and Security Review (2010, Cm 7948)

Security Lancaster http://www.security-centre.lancs.ac.uk/about/


http://www.telegraph.co.uk/sponsored/technology/technology-trends/10231677/cyber-warfare-what-is.html


*The Guardian* (Stuxnet archive) http://www.theguardian.com/technology/stuxnet

*The Guardian* (Snowden archive) http://www.theguardian.com/world/edward-snowden

The Internet of Things Council http://www.theinternetofthings.eu/who-we-are


References

1 Swabey, P. (2013) ‘US Air Force reclassifies cyber security tools as weapons’ *Information Age*
   http://www.wired.com/threatlevel/2012/05/flame/
3 For summary see Tallinn Manual n 6 below at 2. See further Securing Britain in an age of uncertainty: The
   Strategic Defence and Security Review (2010, Cm 7948)
   http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
   ; Australian Cyber Security Strategy (2009)
   http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Pages/default.aspx#h2strategy
   Armed Forces of the Russian Federation in the Information Space’ (unofficial translation available at
   For notification see Atlantic Organisation for Security (2012) ‘Russia’s Cyber strategy Published
   http://www.aofs.org/2012/04/15/russia%2c2%4s-cyber-strategy-published/
6 See n 6 below, at 5
   (Cambridge, CUP)
8 For more on how key terms are used in the report see Glossary to the Report, p 29. The Tallinn Manual
   describes Malware under the slightly broader heading of Malicious Logic (see Tallinn Manual Glossary, 260.)
   (2013) *Cyber War Will Not Take Place* (Oxford, OUP/Hurst)
10 Fulghum, DA., Wall, R and Butler A. (2007) ‘Cyber-combat’s first shot’ *Aviation Week and Space Technology*
   167 (21) 28-31
11 n 9 above, *ibid*
12 *Ibid.* At the time of writing (2014) the dispute between Russia and Ukraine is reported to involve cyber
   operations, however there is no clarity on whether these operations are State-sponsored or down to ‘patriotic’
   ‘Eugene Kaspersky: Russia Ukraine Cyber Attacks Probably Not State Sponsored – CeBIT’

9 Above, ibid; Lindsay, J. (2013) ‘Stuxnet and the Limits of Cyber Warfare’ Security Studies 22 (3) 365-404; Extensive commentary on Stuxnet is available online, see for example archive content at The Guardian http://www.theguardian.com/technology/stuxnet


9 Above, ibid


On Internet of Things see The Internet of Things Council http://www.theinternetoftthings.eu/who-we-are

Metcalfe’s Law proposes that the value of a communications network is proportional to the square of the number of its users (Briscoe, B, Odlyzko A and Tilly B 2006) however, the law is not without its critics, see further Briscoe, B., Odlyzko A and Tilly B. (2006) IEEE Spectrum ‘Metcalfe’s Law is wrong’ http://spectrum.ieee.org/computing/networks/metcalfes-law-is-wrong


See n 3 above, Securing Britain in an age of uncertainty: The Strategic Defence and Security Review (2010, Cm 7948)


Information on Snowden is readily available online, see for example archive at The Guardian http://www.theguardian.com/world/edward-snowden


33 Nicaragua v USA 1986 ICI Rep 14


35 Discussion of International Humanitarian Law can generally be found in texts on International Law, see for example in Dixon n 32 above, see also Turns, D. ‘The Law Of Armed Conflict (International Humanitarian Law)’ in Evans n 32 above, 814-846. For collected legal documents on International Humanitarian Law see Roberts, A and Gueff, R. (eds) (2000) Documents on the Laws of War 3rd Ed (Oxford, OUP)


37 For a reappraisal of the character/classification of armed conflict see Wilmshurst, E. (ed) (2012) International Law and the Classification of Conflicts (Chatham House/Oxford, OUP); on the significance of the classification of armed conflicts see Akande, D. ‘Classification of Armed Conflicts: Relevant Legal Concepts’ in Wilmshurst (op cit)

38 Compare the arguments of the ICRC who suggest that the absence of a threshold is preferable, in that it avoids potential controversy over whether the requisite degree of intensity has been reached: ICRC 31st International Conference of the Red Cross and Red Crescent, Report, International Humanitarian Law and the challenges of contemporary armed conflicts (Geneva, 2011) http://www.icrc.org/eng/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-en.pdf ; see also discussion in Akande, n 37 above


40 Ibid

41 See further discussion in Garraway, n 36 above, Corn, n 39 above, Ratner, S. (2002) ‘Jus ad Bellum and Jus in Bello after September 11’ The American Journal of International Law 96 (4) 905-921; Akande, n 37 above

42 See further Garraway, n 36 above

43 Ibid.


47 Rid, n 9 above

48 See http://www.chathamhouse.org/about-us/chathamhouserule


50 For the expansion of HR liability more generally in combat contexts see the recent decision in Smith v The Ministry of Defence [2013] UKSC 41

51 For the mission statement of Security Lancaster, see http://www.security-centre.lancs.ac.uk/about/
# Appendix: Figure 2 source data

<table>
<thead>
<tr>
<th>Year</th>
<th>Significant cyber incidents</th>
<th>Domestic policy development</th>
<th>International conferences, significant publications and legislation</th>
<th>International policy development</th>
</tr>
</thead>
<tbody>
<tr>
<td>1982</td>
<td>Alleged Russian Pipeline explosion</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2000</td>
<td>Moonlight Maze</td>
<td></td>
<td>The Information Security Doctrine of the Russian Federation</td>
<td></td>
</tr>
<tr>
<td>2001</td>
<td></td>
<td>Budapest Convention on Cybercrime</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2005</td>
<td>Titan Rain</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2007</td>
<td>Cyber attack on Estonia</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2007</td>
<td>Cyber attack on Syria</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2008</td>
<td>Cyber attacks on Georgian websites</td>
<td></td>
<td>Estonian Cyber Security Strategy</td>
<td></td>
</tr>
<tr>
<td>2009</td>
<td>DDoS attacks against governmental, media and financial websites in US and S Korea</td>
<td>United Kingdom Cyber Security Strategy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2010</td>
<td>Discovery of Stuxnet Malware and Operation Aurora</td>
<td>Strategic Defence and Security Review initiates £650M National Cyber Security programme (later rising to £860M)</td>
<td>NATO Lisbon Summit identifies cyber domain as significant Security Risk</td>
<td>Canadian Cyber Security Strategy</td>
</tr>
<tr>
<td></td>
<td>Pakistani ‘Cyber Army’ hack Indian Central Bureau of Investigation website</td>
<td></td>
<td>Japanese Information Security Strategy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Indian ‘Cyber Army’ hack Pakistan Army and governmental websites</td>
<td></td>
<td></td>
<td>South African Cyber Security Policy</td>
</tr>
<tr>
<td></td>
<td>US Dept of Defence admit its internet traffic was rerouted via China for a short period</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Google announce attacks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Year</td>
<td>Event/Report</td>
<td>Conference/Strategy/Resolution</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td>Japanese governmental and defence contractor websites targeted by cyber attacks</td>
<td>United Kingdom Cyber Security Strategy; London Conference on Cyberspace; Australian Cyber Security Strategy</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>East West Institute Russia-US Bilateral on Critical Infrastructure Protection publication ‘Working Towards Rules for Governing Cyber Conflict’; Columbian Policy Guidelines on Cybersecurity and Cyberdefence</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>Discovery of Flame Malware</td>
<td>Budapest Conference on Cyberspace; Conceptual views on the Activities of the Armed Forces of the Russian Federation in Information Space (unofficial translation); National Cyber Security Framework Manual (NATO CCD CoE); Austrian Cyber Security Strategy</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Swiss Cyber Security Strategy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Year</td>
<td>Event 1</td>
<td>Event 2</td>
<td>Event 3</td>
<td>Event 4</td>
</tr>
<tr>
<td>------</td>
<td>------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Snowden revelations</td>
<td>Joint Cyber Reserves open for recruitment</td>
<td>Seoul Conference on Cyberspace</td>
<td>Hungarian National Security Strategy</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>EU Directive on Attacks against Information Systems</td>
<td>Indian Cyber Security Strategy</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>University of California Institute on Global Conflict and Co-operation Workshop Report on China and Cybersecurity</td>
<td>Kenyan Cyber Security Strategy (pending)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Montenegrin Cyber Security Strategy (pending)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Ugandan Cyber Security Strategy (pending)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>NATO annual cyber security exercise now largest of its kind – over 27 countries and partners participate</td>
</tr>
</tbody>
</table>

Endpapers: Author bio

Principal Author: Dr Bela Bonita Chatterjee

Dr Chatterjee is a Lecturer at Lancaster University Law School and an associate of Security Lancaster. Her work concentrates on interrogating transdisciplinary aspects of cyber law. Her most recent work investigates the intersections of international law and cyber conflict.

Conference Confederates

Dr Mark Lacy

Dr Lacy is a Lecturer in the Department of Politics, Philosophy and Religion at Lancaster University with specialisms in politics and international relations. He is the theme lead for Security Futures, an interdisciplinary space to examine the ethical, economic, legal and technical implications of new technologies with the aim of identifying new areas of research and to examine the optimism or fear in debates over emerging trends and moral panics about new technologies. Dr Lacy is also the lead editor of the Routledge book series, Conflict, Security and Technology

Dr Jackson Maogoto

Dr Maogoto is a Senior Lecturer in Law at the University of Manchester. His teaching and research interests are in Public International Law, Jurisprudence and Human Rights. His international law interests encompass the fields of international criminal law, international humanitarian and human rights law, use of force and peacekeeping, space law, counter-terrorism and private military corporations.

Dr Daniel Prince

Dr Prince is a Teaching Fellow at Lancaster University and has been working in the area of mobile network systems and information security for 6 years. He now lectures in information security risk management, penetration techniques and digital forensics as part of the MSc in Cyber Security at Lancaster University, for which he is the course director.
Dr James Summers

Dr. Summers is a Lecturer at Lancaster University Law School. His research interests lie generally in international law and its construction. He has particular interests in the field of peoples' rights, self-determination and statehood and the related cross-disciplinary topic of nationalism. He also has interests in the use of force and the laws of war, in international organisations and international environmental law.

Lt. Cdr. Adrian ‘Tel’ Venables

Lt. Cdr. Adrian 'Tel' Venables joined the Royal Naval Reserve following 24 years in the regular Service during which he qualified as a Principal Warfare Officer specialising in Communications, Electronic Warfare and Intelligence. In addition to a national role in the RNR in establishing a new Cyber Reserves cadre, he is also a self-employed consultant to the MoD advising on cyber security and the development of Command and Control systems. He is also currently studying for a PhD in developing a measurement of national cyber power, which will be his 6th computing and technology based degree.
We wish to thank Security Lancaster for providing the funding for the initial Workshop. We are also grateful to Dr Daniel Prince for consultancy and support, and to Professor James A. Sweeney for invaluable discussion. We express our gratitude to Lt. Cdr. Adrian ‘Tel’ Venables and the Defence School of Policing and Guarding for their generous hospitality, and our thanks to the various attendees on the day – academic and non-academic - for their invaluable contributions and expertise.

This publication has been prepared for general guidance on matter of interest only, is given without responsibility and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, Lancaster University, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequence of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

Copyright Lancaster University © 28/07/2014