Armageddon and the Cyberghost

Cyber-attacks as acts of war

A lecture for Gresham College

28 May 2013

Armageddon and the Cyberghost

The cyber-ghost instils superstition in those who fear the unknown and are sceptical of its existence; the absence of physical evidence makes it difficult to conceptualise the magnitude or severity of the invisible threat.... Armageddon represents the "end of days" the destruction or abandonment of the worldwide web.....

As a global civilisation we rely on a world of connectivity characterised by social media and universal mobile communication in a way inconceivable 10 years ago. In Africa the use of mobile phones to make payments is a new currency; satellites map the terrain, monitor movement, watch and provide connectivity to every corner of the globe, providing communication navigation and intelligence.

Nation states use digital media and technology to mange the administration of government, management of critical infrastructure, defence, food-production and engagement with individual. Most of us never really understand how this connectivity works, with whom we are communicating or the scale of the digital footprint that we are creating. We do not see and cannot conceptualise the menace of cyber-attacks. The echo of cyber-aggression is measured by the billion-dollar defence business grown around it.

In the early 19th Century, the birth of the colonial empires created vast merchant and naval shipping fleets. Private commercial shipping existed alongside the weapons of international expansion and power. The state's commitment was to defend the commercial assets of the countries they colonised and to maintain international trade along the shipping routes in a similar way that we keep the digital communication channels open and accessible. The consequence of not doing so in a world reliant on connectivity is the Armageddon we fear.

In the virtual world, not-knowing whom the aggressor is combines with an absence of physical presence defining either the aggressor or a location where the effect is felt, limits the scope for pursuing legitimate legal counter measures.

Furthermore the distinction between the legal rights of the state and the rights of the individuals to respond to cyber-aggression has yet to be defined much less tested in national or international courts.

The Internet carries more valuable communication, including data and payments information than was ever carried by the ships that fed the industrial revolution. The cyber-highway and the control of infrastructure social media bind elements of society together and have simultaneously removed the control of communication from government.

The Budapest Convention established a common legal framework for the criminalisation (within Europe)for the misuse of computers divided into; Data interference, System interference, misuse of devices, computer-related offences; computer-related forgery, computer-related fraud, content-related offences

1 The Internet as a weapon.

Free access to the digital conduit is a tool for prosperity and social cohesion and is now being considered as a fundamental right. The same digital highway is also capable of being the conduit for malice, criminality and aggression between sovereign states. In the wrong hands the connectivity between diverse databases and control systems has the

potential for totalitarian control. The benefits of connectivity are in quite capable of being the tools of repression.

The viral growth of connectivity now facilitates the aggregation and analysis of unstructured data and information to a degree never previously dreamt of. Combining multiple sources of information facilitates a very detailed profile of the action of states, the effect of weather, movement of populations and the impact of government action, performance of financial market, as well as individual's daily routines, earning, spending (and hence cultural preferences), and associations; the list is endless and connectivity is facilitating viral growth. As we do not yet understand the true limits of this connectivity or information it might disclose, its is impossible to say whether providing universal access via the neural pathways of the internet is a mechanism for good or ultimately and instrument of tyranny.

What started out as a communication protocol now facilitates the remote integration of satellite radar, command and control systems, manages tax, social security, health transport and even food and fuel distribution? The remote management of the instruments of war is just one aspect of digital communications and yet according to the United States National Security Office;

> *…..a significant cyber attack will occur and that it will have lasting implications.*

To what extent is the potential misuse of the Internet subject to the sanction of public or private international law? If the digital highway were to be used as a conduit for acts of aggression what treaties, charters or laws could be invoked to legitimise defensive measures or to justify a counterattack? Semantec, in its 2013 Annual report predicts the increase of state sponsored cyber-attacks.

The prosecution of DDoS and computer worm attacks poses serious challenges to most national criminal law systems. These attacks do not involve any physical impact on computer systems. Apart from the basic need to criminalise web-based attacks[2], the question of whether the prevention and prosecution of attacks against critical infrastructure needs separate supranational legislative continues to be the subject of debate, as does the need for a specific extension to the UN Charter to assimilate the sanctions for cyber-warfare with those for physical aggression.

The rights of a sovereign states to defend themselves against aggression and to take counter-measures is legitimised by international conventions and treaties, developed as result of the world wars. The United Nations Charter proscribes when one state may use force against another. The evolving question is however the extent to which private businesses can lawfully execute positive counter-measures against the originators of cyber attacks based in the territory of a foreign sovereign state.

> *Over the last two decades, the Internet and more broadly cyberspace has had a tremendous impact on all parts of society. Our daily life, fundamental rights, social interactions and economies depend on information and communication technology working seamlessly. An open and free cyberspace has promoted political and social inclusion worldwide; it has broken down barriers between countries, communities and citizens, allowing interaction and sharing of information and ideas across the globe; it has provided a forum for freedom of expression and exercise of fundamental rights, and empowered people in their quest for democratic and more just societies - most strikingly during the Arab Spring* [1]

In the wrong hands the combination of "big data" and the connectivity of the digital network is also the greatest possible tool for humanitarian good or the worst weapon of totalitarian power the world has ever faced.

---

1 Joint communication to the European Parliament, the council, The European Economic and social committee

Confidence in the legitimacy and benign universality of digital connectivity is fundamental to the growth of the digital economy[2]. Whether they are legitimate transactions or crimes the absence of human interaction changes the moral imperative.

This system is under attack, and all of those connected to it are at risk. The computer worm SQL Slammer was estimated to have infected 90 per cent of vulnerable computer systems within the first 10 minutes of its distribution.[3]

The financial damage caused by virus attacks in 2000 was estimated to amount to some 17 billion USD. In 2003 it was still more than 12 billion USD.[4]

By early 2013, Semantec predicted an increase in State-sponsored Cyber Attacks;

> *"The last few years have seen increasingly sophisticated and widespread use of cyber attacks. In peacetime, they provide plausible deniability; in wartime, they could be an essential tool.*
>
> *Cyber attacks will continue to be an outlet where tensions between countries are played out. Moreover, in addition to state-sponsored attacks, non-state sponsored attacks, including attacks by nationalist activists against those whom they perceive to be acting against their country's interest, will continue.*
>
> *Security companies and businesses need to be prepared for blowback and collateral damage from these attacks and, as ever, they need to make strenuous efforts to protect themselves against targeted attacks of all kinds."*

Sophisticated Attack Techniques Trickle Down

> *"Know-how used for industrial espionage or cyber-warfare will be reverse-engineered by criminal hackers for commercial gain. For example, other malware authors will exploit the zero-day exploits used by the Elderwood Gang. Similarly the "open-sourcing" of malware toolkits such as Zeus (also known as Zbot), perhaps in an effort to throw law enforcement off the trail of the original authors, will make it easier for authors to create new malware".*

Websites Will Become More Dangerous

> *Drive-by infections from websites will become even more common and even harder to block without advanced security software. Criminals will increasingly attack websites, using malvertising and website attack kits, as a means of infecting users. Software vendors will come under pressure to increase their efforts in fixing vulnerabilities promptly. Users and companies that employ them will need to be more proactive about maintaining their privacy and security in this new social media world.*

Social Media Will Be a Major Security Battleground

> *Social media websites already combine elements of an operating system, a communications platform, and an advertising network. As they go mobile and add payment mechanisms, they will attract even more attention from online criminals with malware, phishing, spam, and scams. Traditional spam, phishing, and malware will hold steady or decline somewhat; however, social media attacks will grow enormously. As new social media tools emerge and become popular, criminals will target them. Further, we think that the intersection of smartphones and social media will become an important security battleground as criminals target teenagers, young adults, and other people who may be less guarded about their personal data and insufficiently security-minded to protect their devices and avoid scams.*

Attacks Against Cloud Providers Will Increase

---

2 http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf

3 http://news.bbc.co.uk/1/hi/technology/2693925.stm

4 Source Semantec 2013 Annual report

So far, the very big data breaches have occurred in businesses that collect a lot of personal data, such as healthcare providers, online retailers or games companies. In 2013 we expect to see a variety of attacks against cloud software providers.

Increasingly Vicious Malware

Malware has advanced from being predominantly about data theft and botnets (although both are still very common) through fake antivirus scams to increased ransom-ware attacks in 2012. We expect to see these attacks become harder to undo, more aggressive, and more professional over time. Once criminals see that they can get a high conversion rate from this kind of extortion, we may see other manifestations, such as malware that threatens to and then actually deletes the contents of your hard disk. This was the case of the Shamoon attacks that occurred in August and erased data from the infected computer. Essentially, if it is possible, someone will try it; if it is profitable, many people will do it.

The right to retaliate;

WASHINGTON — With President Obama preparing for a first meeting with China's new president, a commission led by two former senior officials in his administration will recommend a series of steps that could significantly raise the cost to China of the theft of American industrial secrets. ***If milder measures failed, the commission said, "the United States should consider giving companies the right to retaliate against cyber-attackers with counter-strikes of their own.[5]"***

"China is two-thirds of the intellectual property theft problem, and we are at a point where it is robbing us of innovation to bolster their own industry, at a cost of millions of jobs," Mr. Huntsman said, with a bluntness that would have been forbidden when he served in Beijing. "We need some realistic policy options that create a real cost for this activity because the Chinese leadership is sensitive to those costs."

"If counterattacks against hackers were legal, there are many techniques that companies could employ that would cause severe damage to the capability" of the Chinese or other groups committing computerized theft, the report said. But it added a qualifier: "while properly empowered law enforcement authorities are mobilized." ***Many in the administration have opposed such ideas, fearing that they could lead to a cycle of escalation between the United States and other nations that could easily spin out of control.***

2 Moving towards Armageddon.

If the scale of cyber-attacks launched from rogue states and territories where the sovereign government condone attacks, at what point does the victim state become entitled to launch counter offensive operations.

In 2009 a group of international experts met to consider the extent to which existing public international law applied to cyber-warfare, and indeed what constituted cyber-warfare, what resulted was the Tallinn Manual.

The manual sought to distil a number of "rules" from the existing international laws as they could be applied to the rights of sovereign states to respond to acts of cyber-aggression by states.

The right to self defence arises if there has been and "armed attack"…. The UN Charter Provides

Article 51

[5] News Analysis: In Cyberspace, New Cold War (February 25, 2013)

Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.

We should be under no allusion that the evolving nature of cyber-attacks and defence constitute a new paradigm in international conflict, as to what may constitute a "just war" in Cyberspace.

Jus ad bellum

….political leaders are the ones who inaugurate wars, setting their armed forces in motion, they are to be held accountable to jus ad bellum principles. If they fail in that responsibility, then they commit war crimes. In the language of the Nuremberg prosecutors, aggressive leaders who launch unjust wars commit "crimes against peace." What constitutes a just or unjust resort to armed force is disclosed to us by the rules of ***jus ad bellum****. Just war theory contends that, for any resort to war to be justified, a political community, or state, must fulfill each and every one of the following six requirements:*

1. Just cause. *A state may launch a war only for the right reason. The just causes most frequently mentioned include: self-defence from external attack; the defence of others from such; the protection of innocents from brutal, aggressive regimes; and punishment for a grievous wrongdoing, which remains uncorrected.*[6]

2. Right intention. *A state must intend to fight the war only for the sake of its just cause. Having the right reason for launching a war is not enough: the actual motivation behind the resort to war must also be morally appropriate. Ulterior motives, such as a power or land grab, or irrational motives, such as revenge or ethnic hatred, are ruled out. The only right intention allowed is to see the just cause for resorting to war secured and consolidated. If another intention crowds in, moral corruption sets in. International law does not include this rule, probably because of the evidentiary difficulties involved in determining a state's intent.*

3. Proper authority and public declaration. *A state may go to war only if the decision has been made by the appropriate authorities, according to the proper process, and made public, notably to its own citizens and to the enemy state(s). The "appropriate authority" is usually specified in that country's constitution. States failing the requirements of minimal justice lack the legitimacy to go to war.*

4. Last Resort. *A state may resort to war only if it has exhausted all plausible, peaceful alternatives to resolving the conflict in question, in particular diplomatic negotiation. One wants to make sure something as momentous and serious as war is declared only when it seems the last practical and reasonable shot at effectively resisting aggression.*

5. Probability of Success. *A state may not resort to war if it can foresee that doing so will have no measurable impact on the situation. The aim here is to block mass violence, which is going to be futile. International law does not include this requirement, as it is seen as biased against small, weaker states.*

6. Proportionality. *A state must, prior to initiating a war, weigh the universal goods expected to result from it, such as securing the just cause, against the universal evils expected to result, notably casualties. Only if the*

[6] Orend, Brian, "War", The Stanford Encyclopaedia of Philosophy (Fall 2008 Edition), Edward N. Zalta (ed.), URL = <http://plato.stanford.edu/archives/fall2008/entries/war/>.

benefits are proportional to, or "worth", the costs may the war action proceed. (The universal must be stressed, since often in war states only tally their own expected benefits and costs, radically discounting those accruing to the enemy and to any innocent third parties.)

3 What constitutes an "armed attack".

The question as to what constitutes and "*armed attack'* was considered in the Nicaragua Judgement of the International Court of Justice.[7]

The experts at Tallinn concluded that the right to employ force in self-defence extends beyond "kinetic attacks" to those that are perpetrated entirely through cyber operations. The International Court of Justice has opined that. "*the means of attack is immaterial as to whether an operation qualifies and an armed attack".*[8]

The *threat* to use nuclear weapons has therefore been held to be an "armed attack" which satisfies the definition that justifies retaliation.

UN Charter Article 2

2.4 All Members, in order to ensure to all of them the rights and benefits resulting from membership, shall fulfill in good faith the obligations assumed by them in accordance with the present All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.

Cyber-operations may therefore be a breach of international law, without necessarily amounting to and "*armed attack".* Only if the level of the cyber-attack reaches the level of an armed attack is the State entitled to respond using force in self-defence.

The International Court in the Nicaragua Case considered the scope of what constitutes "armed force"[9]

Para 191. As regards certain particular aspects of the principle in question, it will be necessary to distinguish the gravest forms of the use of force (those constituting an armed attack) from other less grave forms. In determining the legal rule which applies to these latter forms, the Court can again draw on the formulations contained in the Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations (General Assembly resolution 2625 (XXV), referred to above). As already observed, the adoption by States of this text affords an indication of their opinio juris as to customary international law on the question. Alongside certain descriptions which may refer to aggression, this text includes others which refer only to less grave forms of the use of force. In particular, according to this resolution:

'Every State has the duty to refrain from the threat or use of force to violate the existing international boundaries of another State or as a means of solving international disputes, including territorial disputes and problems concerning frontiers of States.

States have a duty to refrain from acts of reprisal involving the use of force.

Every State has the duty to refrain from any forcible action which deprives peoples referred to in the elaboration of the principle of equal rights and self-

---

7 Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v US) 1986 ICJ 14 (27th June)

8 Legality of the threat or use of Nuclear Weapons Advisory Opinion 1996 ICJ 226 (08th July)

9 Judgment Present: President NAGENDRA SINGH; Vice-President DE LACHARRIERE; Judges LACHS, RUDA, ELIAS, ODA, AGO, SETTE-CAMARA, SCHWEBEL, Sir Robert JENNINGS, MBAYE, BEDJAOUI, NI, EVENSEN; Judge ad hoc COLLIARD; Registrar TORRES BERNARDEZ.

determination of that right to self-determination and freedom and independence.

Every State has the duty to refrain from organizing or encouraging the organization of irregular forces or armed bands, including mercenaries, for incursion into the territory of another State.

Every State has the duty to refrain from organizing, instigating, assisting or participating in acts of civil strife or terrorist acts in another State or acquiescing in organized activities within its territory directed towards the commission of such acts, when the acts referred to in the present paragraph involve a threat or use of force.'

Unsurprisingly the experts who met at Tallinn were not unanimous as to what form of cyber attack was sufficiently serious to constitute and "*armed attack".* The group debated whether this requires serious personal injury such as that caused by an attack on the control mechanism of a water supply would be such an attack or whether financial loss alone was sufficient to meet the threshold, or indeed whether the accumulation of a series of pin-pricks could do so. The International Group of Experts at Tallinn did agree however that a devastating cyber-attack undertaken by a group of terrorists from within State A against the critical infrastructure located in State B would constitute as an armed attack by those cyber-terrorists against State B.[10]

The one cyber-attack the International Experts agreed was being capable of categorisation as an "*armed attack"* was the deployment of the Stuxnet virus which disabled the Iranian centrifuges (part of their nuclear program).[11]

3.1 Prevention of escalation.

The reluctance of the International Experts to define what constitutes and *armed attack* in the context of cyber-warfare is entirely understandable. The words themselves were not coined to deal with digital incursions.

There seems to be little doubt that we are moving into an era when a state's frustration, financial cost and the fear of imminent irremediable loss could easily boil over into both kinetic and non-kinetic retaliation. The signs are all to clear to see

Gen. Keith Alexander, director of the National Security Agency (15th March 2013) [12] said cyber warfare "teams" would be ready by 2015)

*Let me be clear, **this defend-the-nation team is not a defensive team**; this is an offensive team that the Department of Defense would use to defend the nation if it were attacked in cyberspace," he said during the testimony.*

Citing "destructive" cyber attacks on the Saudi Aramco oil company last summer, during which 30,000 company computers were damaged, Alexander said experts believe the threat of attack will grow, and "there's a lot that we need to do to prepare for this

On 17th May 2013 the Obama administration declared;

China's government must take action to stop the "unprecedented" wave of Chinese cyber-attacks against the US, President Barack Obama's most senior security aide said on Monday

He urged Chinese officials to show "recognition of the urgency and scope of this problem and the risk it poses – to international trade, to the reputation of Chinese industry and to our overall relations".

---

10 . Ultimately it will be for the International Court to decide.

11 Widely believed to have been created by the CIA.

12 In testimony before the Senate Armed Services Committee

4 The International Court and a new UN Convention or Protocol.

Within Europe the adoption of the Budapest Convention represents a common standard for criminalisation of cross border attacks. To date the dominant response to cross border cyber-attacks has been defensive especially (but not exclusively) where those attacks emanate from outside of Europe.

It is not always clear whether cyber attacks have been state sponsored or condoned. Private international law is an expensive and ineffective weapon against the cyber-ghost unless there is a clear obligation and incentive on the part of the host state to investigate disclose the source impose sanctions for such attacks and enable the victims to obtain compensation.

It is entirely conceivable, that the identifiable source of cyber-attacks will be vulnerable to kinetic and non-kinetic retaliation sooner rather than later, leading to a round of escalation and protectionism which could destroy the many benefits which global cyber connectivity brings.

Each state must take direct responsibility for those whom it governs and who connect to the world-wide-web. A failure to do so risks escalation and even partitioning of the network. Whilst this may be unfamiliar territory the International Court has a significant role to play in establishing the responsibility of States to one another in Cyberspace.

The Tallinn Manual provides a rigorous structure that not only demonstrates where the existing public international law provides a response to these challenges; it exposes the shortcomings of the existing public international infrastructure.

Whilst existing laws were defined by the horrors of world wars and conflicts we hope will never return there must be a credible risk that failing to provide a new legal infrastructure that is fit for purpose in the cyber-age risks individuals, commercial enterprises and states taking unilateral and unregulated action creating a cycle of escalation and "Armageddon in Cyber-Space", "the end of days". It is not inconceivable that an attack or the retaliation to an attack could cause uncontrollable escalation and even conventional conflict.

The International Court of the United Nations has a dual jurisdiction: it decides, in accordance with international law, disputes of a legal nature that are submitted to it by States (jurisdiction in contentious cases); and it gives advisory opinions on legal questions at the request of the organs of the United Nations or specialized agencies authorized to make such a request (advisory jurisdiction), but as observed by Judge Stein Scholberg[13]….

> *"In-order to establish Criminal offences in Cyberspace provisions must be enacted with as much clarity and specificity as possible and not rely on the vague interpretations of existing laws. When cybercrime laws are adopted perpetrators will be convicted for their explicit acts not by existing provisions stretched in the interpretations, or by provisions enacted for other purposes covering only incidental peripheral acts.*

There are of course international conventions including the European Convention on Cybercrime but what these do not adequately address is the situation in which a nation state has neither the genuine will to investigate nor means to prosecute attacks which emanate from its sovereign territory.

Whilst the private national laws, driven by international treaty have evolved language, which provides both civil and criminal remedies, the public international law has not. Allowing or threatening launching a physical armed attack on another state from one's

[13] Twelfth United Nations Congress on Crime Prevention and Criminal Justice 23rd March 2012

own territory is capable of constituting an attack by the host state justifying a proportionate retaliation.

Whilst there is language in the UN charter is capable of being construed to cover cyber-attacks but the uncertainty and lack of specificity is undesirable and may encourage or at least fail to discourage States from allowing their government and non-government resources from launching attacks.

Judge Stein Schjolberg (Court of Appeal Norway) has continued to develop proposals for an international tribunal under the auspices of the International Criminal Court to prosecute cyber-crime[14] having recently published the second edition of those proposals.

This may indeed be one route that can be taken, but it faces a number of significant hurdles. The first is the relatively simple first step of ensuring universal international criminalisation of attacks on foreign critical infrastructure and the second, backing this with a clear legitimisation for commercial sanctions or remedies against the host State for the benefit of the State and its citizens in which the affected assets are located. The rationale for the International Criminal Court was that the states where the crimes were committed were either unwilling or unable to prosecute them. The evidence cited above tends to show that it is the States unwillingness or positive encouragement to the attackers underpins major attacks.

The response to state sponsored (which includes condoning) cyber-piracy, is as the news reporters have identified, politically and diplomatically sensitive. With the danger of escalation into trade wars, protectionism and even kinetic exchanges ever present it is doubtful that offending countries will give-up the instruments of cyber-warfare that reside on their sovereign soil, or that they will recognise an international tribunal unless cyber-warfare is brought within the rubric of conventional armed conflict.

Until an adequate response can evolve or perhaps there is a crisis which threatens the peace and security of nations, or the freedom to trade it is unlikely that a new protocol to the UN Convention will become a reality at least in the short term, but it is certainly an objective to which all states should aspire.

The predicted increase in state sponsored cyber-attacks has resulted in a corresponding increase in the potential victims reaching for cyber-insurance to supplement substantial expenditure on technical defences. Organisation which hold substantial data on individuals face a triple risk of; damage to their ability to trade, damage to reputation and substantial fines by the regulatory authorities.

The Launch of the "EU Cybersecurity plan to protect open internet and online freedom and opportunity" is a clear recognition of the need engage all of the stakeholder and to develop a public international infrastructure to protect access to the Internet as a fundamental right.

An international imperative and recognition of the need to impose State responsibility on is citizens will avoid Armageddon provided that those mechanisms are implemented and are technology neutral.

Thank you

Alexander Carter-Silk

14 (Proposal for International Criminal Court for Cyberspace)