Cyber security, diplomacy and international law

by Charles Chatterjee and Anna Lefcovitch

1. INTRODUCTION

Over the last decade or so cyber security has attracted the attention of many communities/ professions, in particular, the business community, the community of diplomats, and various public departments, including those for military/defence and security departments. This issue of poaching security-related information has remained with us since Graham Bell invented telephones, although at that time cybercrimes did not exist. The most appropriate term would be "cyber insecurity" as technology, when abused, takes away security or de-stabilises security systems. Cyber insecurity is created by technological devices, usually with the help of robots.

It has to be seriously considered whether cyber security/ insecurity may be effectively dealt with only by law. It is an issue which entails a number of other related matters, namely, espionage as an identified technique of poaching information; misconduct on the part of the insiders; high technology; and competition in cyber-based activities which offer financial gains and which often form the basis for transnational terrorist activities.

The primary cause of cyber insecurity may not necessarily be any of the issues mentioned above; the most important cause for cyber insecurity seems to be unnecessary warfare, often based on unjustifiable reasons which prompt the people concerned to take revenge on the initiators of wars. War begets war.

Cyber-attacks often become possible owing to the collaborative work done by "insiders", that is employees who decide to facilitate disclosure of information. Some examples of cyber-attacks in recent months and years are well-known. Cyber-attacks are performed with the aid of technology, but the prime movers of these attacks are human beings. People working for intelligence or intelligence-related departments need to be subject to controls.

An assumption exists, particularly in the developed West, that developing countries in general lack the capabilities for cyber-attacks because they do not have the sophisticated technology required to make them. This assumption has been challenged in recent times because US security systems have been subject to successful cyber-attacks by external bodies from non-Western sources. Furthermore, some developing countries do already possess both the very sophisticated technology capable of carrying out such attacks and sophisticated intelligence systems. If urgent international actions are not taken on this issue, there will be even more cyber warfare between countries, the consequences of which are very clear. Instead of spending very large amounts of money to develop even more sophisticated technology, the time has now arrived to abandon cyber warfare through negotiations and international co-operation.

This article does not pretend to offer any remedies for cyber warfare; its principal aim is to re-affirm that peace must be brought about by peaceful means rather than warfare. Attacks entail counter-attacks, intrusion or intervention, be it called humanitarian or otherwise, which will lead to counter intrusion or intervention in others' affairs. Foreign policy-making by states seems to have tilted towards security issues, rather than friendly relations between states through trade and investments which should, in turn, lead to socio- economic development.

As cyber security is partly an "insider job", much work is required by both rich and poor countries on this issue to criminalise such actions, and also by pro-active international action through co-operation leading to binding international conventions in order to designate cyber warfare as "prohibited acts", and to make it a "peremptory norm". Cyber threats can take various forms, such as cyber warfare, cyber terrorism, espionage, and hacking. These threats are primarily politically motivated; on the other hand, cyber threats can also be financially motivated, such as intellectual property threat, fraud, and hacking for the purpose of creating fear or retribution.

The primary objective of politically-motivated attacks is generally to disrupt services, particularly in the public sector. These attacks are usually launched to undermine the perception of the public in regard to their government. Successful attacks on public sector websites can adversely affect trust in government, in consequence of which the public will increasingly develop negative views and become averse to accepting government information. Most non-politically motivated attacks are generally launched for financial gain, and are usually launched for stealing data, credit card information by using existing hardware, or creating or buying hardware on black markets. Incidentally, the term "cyber hackers" refers to

those who aim to damage or destroy a computer network or system (see *Oxford Dictionary of English,* 3rd ed, 2010).

Cyber threats may be internal or external; a cyber threat is internal when it is posed by a current or former disgruntled employee. In the case of Wikileaks, a soldier in the US army downloaded sensitive information to a USB drive with a view to passing it on to others, which he did. The majority of cyber-attacks are "external", and most of the perpetrators of such attacks are motivated to commit those crimes as a revenge on certain state sectors or policies.

The internet was created by the Defence Advanced Research Projects Agency (DARPA), a US government entity commissioned to develop innovative technology for the military, but it did not remain confined to military affairs alone and the system was eventually made available to the entire world. By the time President Clinton and Vice-President Al Gore came to power in 1993, the US private sector became an information age sector. In his attempt to reinvent the US Government, Vice-President Gore brought the internet into global use and the benefits of information technologies to the public sector for the purpose of greater productivity, and to reduce the costs of dealing in information. The term "electronic government" or "e-government" was born (for a good discussion of the various aspects of cyber security, see K Andreasson (ed) *Cybersecurity: Public Sector Threats and Responses,* Boca Raton, CRC Press (2012) at p 112). But the child was allowed to attain its maturity too fast; the public demanded not only an information age, but also the internet transaction age.

Then along came the age of openness, transparency and accountability for governments, particularly in the West. The primary logic behind "open" governments is to observe transparency in actual practice, the very essence of democracy – a government of the people, by the people and for the people. President Obama has been an ardent supporter of free information flow. In the UK, the Hansard Society (see "Digital Dialogue 3") maintains that it is important to have a clear, transparent, and a rule-based accountability for all forms of participation by people and politicians; but such a movement might lead to an encroachment upon privacy and confidentiality. On the other hand, a government may, on the grounds of the national interest, always be intrusive to seek information on people's private lives. Thus, a dilemma arises – what should be the balance between openness and confidentiality?

2. WHY SHOULD CYBER-ATTACKS BE REGARDED AS SERIOUS CRIMES?

The growth of cybercrimes has been increasing since the beginning of the 21st century. These crimes/attacks have primarily taken four forms: (a) physical damage to tangible properties, for example the destruction of aircraft, or dams, or infrastructural damage; (b) psychological damage, such as falsification of websites or disruption of services; (c) financial damage/loss, such as unauthorised access to bank accounts; and (d) invisible damage, which may not be recognised by victims as they are caused by and through covert operations. Each of the types of crimes described above are technology-based; thus attackers can hit their targets with precision, and attain their objectives unless their efforts are foiled by those targets – again with the help of external information usually provided by allies.

Attempts to commit cybercrimes, even if they fail to consummate, are to be treated as criminal acts. The general principles of crime – *mens rea* and *actus reus* – apply to cybercrimes too. Uncertainty exists however about the identity of the criminals. Locations of the crimes may also be difficult to identify. Examples of cyber-attacks are numerous: large scale attacks took place in Estonia in 2007 and Lithuania and Georgia in 2008, and also against South Korea and the US in July 2009. Cyber-attacks have become a daily phenomenon; they are often successful not only because of the application of sophisticated technology, but also they may be facilitated by "insiders". This process is further complicated by the fact that it remains unclear who operates the network – hence the origin of the term "ghost network".

Cyber-attacks can directly affect national security, thus certain authors have suggested that it is necessary to involve intelligence agencies to prevent attacks (see J S Nye, "Cyber Power", Harvard Kennedy School Buffer Counter for Science and International Affairs, May (2010); and M Tsuchiya, *National Security by Intelligence*, Tokyo, Kelo University Press (2007)). However, it must be remembered that attackers appear to have a special level of expertise capable of beating most competent intelligence agencies in the world. It is a war of technology against technology, and the implications should be urgently appreciated by the international community.

Cyber threats are more worrying than actual attacks. They hang over our heads without us knowing in what form or shape they might visit. The internet has many positive and educative aspects, but at the same time it can act like a monster with its negative and destructive dimensions. Richard Clarke, a former US Presidential Adviser said on this matter (in *Cyberwar: The Next Threat to National Security and What to Do About It,* New York, ECCO (2010) at xiii) that "if we could put the genie back in the bottle, we should – but we can't." We are unable to do so for a variety of reasons – abuse of the internet is as popular as its legitimate applications. It is often difficult to teach criminals ethics, and thus we have to learn how to live with cyber threats. According to Nigel Inkster of the Institute for Strategic Studies (IOSS) in London,cyber warfare poses a serious future threat which could have serious implications for all of us (see "Cyber Warfares" CBC Radio "As it Happens", 10 February 2010). Stuxnet (a device for malicious software attacks) is one of the most sophisticated cyber weapons; W J Broad et al "Israeli Test on Worm called Crucial in Iran Nuclear Delay", *New York Times*, 15 January 2011 at 1A.

It is through cyber weapons that the most effective and extensive form of terrorist activities may be carried out.

3. SOME MAIN CAUSES OF CYBER ATTACKS

Cyber-attacks are caused by a variety of factors, some of the most identifiable of which are referred to below.

Lack of public awareness: many users of computers, the internet and even mobile phones and social media fail to realise how by irresponsible use of these technologies they give away many information of a personal nature to others who are abusers of these technologies.

Insiders: these are employees working for national defence or intelligence departments in particular, who give away important security information in exchange of money or other benefits.

Aggressive attitudes/behaviour of certain states or governments: this pattern of behaviour culminates in interconnection in other states or governmental affairs with a view to controlling the conduct of others, which results in counter attacks.

A clear departure from "clean" diplomacy: this has existed for a very long time; and

Competitive high technology-based espionage and hacking: this can be treated as a political game.

Creators of each of these pre-determined causes are human beings.

4. WOULD PUBLIC-PRIVATE PARTNERSHIP REDUCE THE RISKS OF CYBERCRIMES?

The cyber world is, in effect, *terra incognita* – the unexplored territory beyond the boundaries of the known world. It is a territory which is subject to various exploratory activities, primarily for hacking information from others; ironically, exploration of the cyber world may benefit the mankind. Cyberspace is an unchartered sphere dominated by terrorist groups, criminal syndicates, experts in technology and illicit money providers – a perfect club for criminal activities which can belittle governmental efforts to counteract its lawbreaking.

For over 25 years, various US agencies, including Congressional hearings and think tanks, maintained as the private sector was the predominant operator of cyber structure, the formation of a public-private partnership might be useful in acting as a formidable force to fight against cyber hackers/cyber attackers. Little did they realise that the plan was misconceived, and that its enforcement would be fraught with difficulties which emanated primarily from the differing business objectives and strategies of the two sectors. The expectations of private and public stakeholders are also significantly different, with the private sector industries being profit-maximisers. But opposing views were available in the US as to the merits and disadvantages of public-private initiatives.

In 1997, President Clinton appointed the Commission for Critical Infrastructure Protection (CCIP) with the mandate to assess the nature of infrastructure threats posed by cyber attackers. The CCIP's research identified several categories of threats to which not only the US but also many other countries would be vulnerable, including information hacking, economic espionage, cyber terrorism, criminal organisations, national intelligence services, and insiders. It is the insiders who make cyber-attacks easier for attackers, but the question remains how to carry out surveillance over them; furthermore, what preventative measures may an employer take in order to ensure that "insiders" are not created?

The CCIP also emphasised the importance of working with the private sector in the belief that such a partnership would create a formidable platform for combatting cyber-attacks. This view was shared by the Centre for Strategic and International Studies (CCIS) in its report of December 2008, although it identified certain shortcomings – namely the lack of agreements on roles and responsibilities and the benefits of information sharing between the two sectors; see further Centre for Strategic and International Studies, December 2008, "Screening Cyberspace for the 44th Presidency", CSIS. org/files/media/csis/pubs/208 screeningcyberspace_44.pdf pp 43-44.

During the first term of President Obama's office, the White House Cyberspace Policy Review, 2009, pointed out, *inter alia*, that an unclear delineation of roles and responsibilities existed which was rather unhelpful for any joint projects. There were reasons why public-private partnership model may not be the solution:

(i) A public-private initiative would require information sharing between the two parties which neither of the sectors might volunteer; furthermore, private sectors might expose industries to onerous regulations to meet government security requirements. President Clinton was also sceptical about the prospects of working successfully with the private sector in the US (see Presidential Decision 63, 22 May 1998).

Given the fundamental differences between the objectives of the private sector in general, and those of the public sector in particular, it would be difficult to bridge the gap between the two; furthermore, the need for cyber security protection may be perceived differently by the two sectors too. Confidentiality and security are also viewed differently by the two sectors.

(ii) Unless a business community believes in self-regulatory measures (ie which would impact their profit-maximisation policy), there will always remain a degree of "mistrust" towards private sectors. In 2010, for example, the US government proposed the Rockefeller-Snowe Bill with a view to strengthening the position of the government by providing it the authority to direct US infrastructure owners and operators to close down their work in the national interest. But

this treaty fuelled fears in the US private sector that the proposed governmental action would result in adverse business consequences. Such fears, whether real or not, tend to confirm the fear that any attempt to effect a marriage between the two sectors would lead to an expensive divorce. So, the first obstacle to a public-private partnership is the lack of trust between the two parties.

The attitudes of the two sectors toward these issues and problems surrounding cybersecurity need to be seriously considered. Whereas the business community at large would like to take advantage of creative aspects of technology of all types, the public sector has to act as the guardian of national security by minimising abuses of technology.

Espionage on business strategies and public sector secrets are entirely different in nature, and the objectives are also different. Waste costs incurred by businesses will be passed to their customers, but the public sector may not necessarily do so. Furthermore, "hacking" for the purpose of seeking confidential information is often tolerated by business communities, but these incidents are not usually disclosed to the public lest their business reputations are jeopardised. As stated earlier, the public sector ethos is significantly different from that of the private sector. Thus, private sectors may not be very enthusiastic about any co-operation programmes with public sectors.

(iii) Treaties for public-private partnerships are often based on the assumption that not only would their interests coincide but also that a harmonious relationship between the two sectors would be easy to develop; but neither of these assumptions may be confirmed. The infrastructural assets of the public sector are different from those of private sectors. A high degree of uncertainty exists as to whether private sectors would be willing to subject themselves to regulatory measures which may be ordered by the public sector. Cyber insecurity is a problem which should be addressed by both public and private sectors, but the curative and preventive aspects of the problems are viewed from different perspectives. Private sectors may also adopt measures according to the needs of each industry; thus no one formula will fit every industry.

The internet has become an integral part of the contemporary society; perhaps its disadvantages or darker side outstrip its advantages or brighter side. It has been imposed on our daily life activities although most people in the world did not contribute in any way to its invention and uses. Interestingly enough, almost all age groups, whether willingly or unwillingly, tend to abuse this technology.

The dilemma is that it would be foolish to deny the positive sides to this technology. There is a need to reduce abuse of the internet, whether by the public sector or the private sector or by both; on the other hand, perhaps from an emotional point of view it may be stated that not only national societies but also the entire international community should appreciate how the internet could make our lives intolerable. A high degree of public awareness, combined with concerted commitment to action, is essential to minimise the incidence of abuse of the internet.

5. THE CAUSES OF INSECURITY

Use of super-sophisticated technology

Such technology can invade confidentiality by overcoming less sophisticated technology. This gives rise to a technology race, which usually takes place between the rich countries and rich criminal organisations, which seem to have more financial and scientific back-up than the poor countries.

Insiders

It is common knowledge that cyber insecurity is often created by certain employees within a country's security-related institutions. Obviously, for financial greed they transfer their loyalty from their employers to the external providers of "gains", whether financial or otherwise. Despite acceptance by employees of the confidentiality clauses in their contract of employment, breach of these clauses has become a common phenomenon.

Irresponsible use of technology

This can include the use by people of their mobile phones, in consequence of which unwittingly opportunities for abuse/misuse of private information are created for rogues.

Buying and selling of confidential information

This information is usually of a public nature, and the process may be described as another form of "insider dealing".

Espionage

Espionage has been an integral part of diplomacy since the latter first originated out of inter-nations relations in the middle ages, when the concept of "cybercrime" did not exist. As a tool of diplomacy it may be described as "clandestine diplomacy". The forms and applications of espionage have been changing ever since; incidentally, when diplomacy is power-based, as is unfortunately the case now, diplomats are required to change the form to make it negotiation-based, on which rests the true foundation of diplomacy.

6. THE NATURE OF INTERNATIONAL ACTION TAKEN AGAINST CYBERCRIMES

So far international action against cybercrimes has taken the form of recommendations urging governments to take preventive action. The International Telecommunication Union (ITU), a specialised agency of the United Nations which

is primarily concerned with information and communication technologies, is also responsible for the safety of all those who use the internet. The ITU has been dealing with international security issues since its inception in 1865; although the nature of technologies has significantly changed since then (the days of telegraph), the goal remains the same – to forge partnerships with states to create a safe and secure environment. The co-relationship between access to communication and peace and safety cannot be denied. As cyber threats are global, their solution must also be addressed from a global point of view and by global means.

Does the global international community have the capacity to deal with this threat on a united front? Furthermore, do all states accord similar priority to these threats and co-operate and collaborate with other states accordingly? Do all states have the required enforcement capacity whereby any binding international convention may be effectively enforced? There is the other fundamental issue of whether every state would pay equal attention to the need for international co-operation on the basis of what may be described as "functional and shared sovereignty". Many other related issues may be added to this list of questions to ascertain the prospects of enforcing any formula agreed to by the international community. A global framework is needed to tackle a global problem, but one cannot disregard the obstacles involved. In this context, it is also important to emphasise that fraud, theft and forgery exist online just as they do offline; thus, cybercrimes come from two sources which make them even more difficult to deal with successfully.

The inference may be drawn at this stage that one state's superiority over cyberspace and defence against these crimes would not free it from these crimes; it must be prepared to defend itself from attacks from a variety of sources with innovative ideas. Cyber criminals go unpunished even though they commit high crimes. Can ITU alone effectively deal with these crimes? This is not to suggest that ITU is not a useful organisation, far from it, but given the nature of the international community and the pervasive nature of these crimes, ITU needs a high level of co-operation from its Member States.

In this connection, it is worth pointing out that goal number 8 of the Millennium Development Goals of 2000 called for a global partnership with the private sectors to ensure the availability of the benefits of information and communications technology to those who have minimal access to them. This ideology was further re-enforced by holding a two-part World Summit on the Information Society in Geneva in 2003 and again in Tunisia in 2005. At these summits the governments entrusted the ITU to provide the lead to co-ordinate international efforts in regard to cyber security.

Since 2006, the ITU has adopted numerous resolutions, decisions, programmes and recommendations on cyber security; there is no need to go into the details of those instruments other than pointing out that each of them apparently had a separate objective, but the fundamental theme of each carried a similar message. ITU develops tools, based on contributions from its membership, to safeguard its efficiency and security and to promote end-user confidence by dealing with, *inter alia,* spam, cybercrime, and attacks on communication systems.

In May 2007, then ITU Secretary-General launched the Global Cybersecurity Agenda (GCA) primarily with a view to challenging the onward march of cyber-attacks through international co-ordination. GCA was built on five pillars: organisational structures, technical and procedural measures, capacity building, legal measures and international co-operation. But in view of various legal systems in the world, implementation of each of these pillars at a national or regional or an international level will encounter difficulties. In so far as cyber security is concerned, developing countries will take longer than the middle-grade countries to build an acceptable level of capacity, but nevertheless it has to be started.

GCA also prescribed seven strategic goals which ranged from the plan for developing a model to cybercrime legislation; global strategies for the creation of appropriate structures and policies for national and regional organisations on cybercrime; the establishment of a globally accepted minimum security criteria and accreditation schemes for hardware and software systems; a global framework for a vigilance and warning system requiring cross-border co-ordinations; to the development of a global strategy to facilitate human and institutional capacity.

As to legal measures, GCA recommended harmonisation of cybercrime legislation; and where necessary, with the help of ITU. It also recommended the development of a publication entitled "Understanding Cybercrime: A Guide for Developing Countries", in addition to developing a toolkit for cybercrime legislation it also recommended Member States to comply with ITU standardisation work. GCA also emphasised the need for more harmonisation work at a global level for attaining international co-operation. The need for capacity building at all relevant levels across the world cannot be over-emphasised. This hinges on the issue of international co-operation, which the international community hardly manages to achieve, unless one cites examples of international co-operation in respect of the right of innocent passage for the purposes of import-export through territorial waters or airspace, as the case may be. Thus, one should not raise very high hopes that such co-operation would be achievable in eradicating cybercrimes. This issue has been further developed in the conclusions (s 10) of this article.

7. THE EU INITIATIVE

According to EuroAction, an on-line information provider on EU affairs, in early 2010 the European Commission estimated the costs of cybercrime for the EU at €750 billion, which is a staggering amount. The European Union has identifiable programmes against cybercrimes, which have been

published principally in the form of Directives, Regulations, and consultative papers; for example, 2002/21/EC of the European Parliament and of the Council of Ministers of 7 March 2002, (a framework Directive on Electronic Communications Network and Services; Council Regulations on a Collaborative Approach to Network and Information Society (2009/321/01)).

European cyber security policy predominantly focuses on the domains of network and information security and cybercrimes, and to that effect the North Atlantic Treaty Organisation (NATO) formed the Co-operative Cyber Defence Centre of Excellence in Estonia. Within the EU, the Commission and the EU Parliament have taken proactive action in emphasising and encouraging partnerships. The Director General (DG) Information Society and Media, includes, *inter alia*, investigation of security risks in certain types of technology, promotion of critical infrastructure protection, and the nature of awareness amongst users regarding cyberspace risks and digital literacy education in cybersecurity. Based on the documents (Directives, Regulations etc) issued by the European Union authorities one can safely maintain that the EU is fully aware of the nature of cybercrimes and the need for protecting open interest and on-line freedom and opportunity. In the context of this article, there is little point in tracing the history of the EU initiatives on this matter, but some of the most recent initiatives taken by the EU comprise:

(a) the Treaty for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union made by the European Commission on 7 February 2013 (COM (2013) 48 Final/2013/0027 (COD));

(b) Joint Communication to the European Parliament, the Council, the European Economic and Joint Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, dated 7 February 2013, submitted by the High Representative of the European Union for Foreign Affairs and Security Policy; and

(c) Digital Agenda for Europe – the report entitled "Cybersecurity: A Europe 2020 Initiative" dated 28 July 2015.

The 2013 proposed Directive was to be, in reality, a Directive on Network and Information Security (NIS) which aimed to ensure a high level of network and information security across the EU in order to avoid or minimise the risk of major cyberattacks or technical failure of information and communication infrastructures in the Member States. The proposed Directive, which was quite comprehensive in scope, primarily covered the following issues:

- upon implementation, each Member State shall reach a certain level of network and information security, and develop a national cyber security strategy and points of contact for information sharing. Each Member State shall also establish a "competent authority for cyber and a Computer Emergency Response Team (CERT)";
- establishment of an all-EU co-operation plan and early warnings system in order to ensure a EU co-ordinated response for cyber incidents; and
- promotion and adoption of effective risk management practices in both public and private sectors through the introduction of cyber incident reporting in various sectors

In other words, the proposed Directive aimed at ensuring a high common level of network and information security across the EU. This would require Member States to improve their co-operation with each other, but only if each state was similarly equipped to do so – ie capable of adopting appropriate steps to manage security risks and report serious incidents to the national authorities concerned. Dissimilarities in standards of capabilities hinder the creation of trust among the Member States, which is a pre-requisite for co-operation and information sharing; thus, there may be insufficient protection against network and information security across the EU.

Over the last decade or so the EU, as a regional institution, has made particular efforts to combat cyber insecurity; for example, in 2004, the European Community established the European Network and Information Security Agency (ENISA - see Reg (EC) No 460/2004) with a view to developing a culture of NIS within the EU. Furthermore, on 30 September 2010, a Treaty to modernise the mandate of ENISA was adopted (COM (2010) 521), which received the attention of the Council and the European Parliament. On 30 March 2009, the Commission adopted a Communication on Critical Information Infrastructure Protection (CIIP) for protecting Europe from cyber disruptions by enhancing security (COM (2009) 149). This Communication launched an action plan to support Member States' efforts to ensure prevention of cyberattacks, and that plan was endorsed at the Ministerial Conference on CIIP in Tallinn in 2009. On 18 December 2009, the Council adopted a Resolution entitled "A Collaborative European Approach to Network and Information Security" (2009/C 321/01), and in May 2010 the Digital Agenda for Europe (DAE) was adopted, the principal purpose of which was to emphasise the trust and security as fundamental pre-conditions for accepting (information and communications technology (ICT) by the Member States, which would contribute to the objectives of the Europe 2020 Strategy. The Commission's study in 2011 on hacking in the CIIP action plan which was activated in 2009 suggested that a purely national approach to tackling the security and resilient challenges had proved to be insufficient (on 27 May 2011, the Council of European Union stressed the need to make ICT systems and networks resilient and secure against all possible disruptions); in other words, a more co-operative approach across the EU would be essential, but unfortunately this is

where the problem persists.

However, on 11 January 2013 the European Cybercrime Centre was set up as part of the European police Office (Europol) to act as the focal point in the fight against cybercrime in the EU. Computer emergency response teams (CERT-EU) have also been set up by various European institutions and agencies. The EU also works on cyber security at both bilateral and multi-lateral levels. In 2010, the EU-US Working Group on Cybersecurity and Cybercrime was established. The EU is also active in certain multilateral institutions, namely, the organisation for Economic Co-operation and Development (OECD); the UN; the International Communication Union (ICU); the Organisation for Security and Co-operation in Europe (OSCE); the World Summit on the Information Security (WSIS); and the Internet Governance Forum (IGF).

According to Article 114 of the Treaty on the Functioning of the European Union (TFEU), the EU can adopt:

> *... measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internet market.*

Given the transnational dimension of network and information systems, any disruption in one Member State can adversely affect the other Member States and the EU as a whole, including issues such as cross-border movement of goods, services and people. It is to be re-emphasised that an uneven NIS national capabilities, policies and level of protection system across the Member States lend to barriers to the Internet Market.

Thus, in order to tackle the consequences of disparity in NIS national capabilities, EU intervention in NIS plans would be justified by the principle of subsidiarity. A minimum level of NIS capability at a national level would be essential, and perhaps should be activated by obligatory regulatory measures whereby effective protection of fundamental rights and, in particular, the right to the protection of personal data and privacy, may be maintained. It is of course important that in imposing measures on the Member States, the principle of proportionality is also observed, as otherwise small operators (SMEs) would be victims of a disproportionate burden of costs.

The objectives of the proposed Directive may be better achieved at the EU level rather than by the Member States individually. Indeed, the EU may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on the European Union. The Commission may be empowered to adopt implementing acts in accordance with Article 291 of the Treaty on the Functioning of the European Union (TFEU).

There is little point in going into any details at this stage of the Treaty for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union; suffice to say that the Treaty recommends, *inter alia*, the establishment of a co-operation mechanism at Union level with a view to allowing information exchange and co-ordinated detection and response regarding NIS. In order for that mechanism to be effective, all Member States should have the minimum capabilities and strategy to operate NIS in their respective territory; to achieve that, each would be required to take the necessary measures with a view to ensuring the protection of its essential security interests to safeguard public security.

Indeed, under Article 346 of the TFEU, no Member State is obliged to supply information the disclosure of which is considered contrary to the essential interests of its society. The TFEU also recommended the establishment of a body with adequate financial, technical and human resources which would be responsible for considering NIS issues and acting for cross-border co-operation at Union level, in addition to establishing computer emergency response teams which would guarantee effective and compatible capabilities to deal with incidents and risks.

The TFEU also pointed out that a secure and effective co-operation mechanism should enable structured and co-ordinated information exchange, detection and response at Union level (the Treaty, op cit, at 13 but see section 8 of this article on international co-operation). The European Network and Information Security Agency (ENISA) has been entrusted with the task of assisting Member States and the Commission by providing its expertise and advice, and also for facilitating the exchange of best practices.

In an effort to build capacity and knowledge among the Member States, the TFEU further maintains that the co-operation network should also operate as a platform for the exchange of best practices among Member States; it also plans to put a secure information-sharing system in place to allow exchange of sensitive networks. The drafters of the TFEU Treaty believed however that co-operation between the public and private sector would be essential.

Whether any information is "confidential" or not is to be considered in accordance with EU and national rules on business confidentiality; furthermore, a common website is planned to publish non-confidential information on the incidents and risks. It is worth mentioning that notification of an early warning within the network may be required only where the scale and severity of the incident or risk concerned "... may become so significant that information or co-ordination of the response of Union level" would be necessary.

The TFEU has also identified the need for closer international co-operation to improve security standards and information exchange, and for the promotion of a common global approach to NIS issues, but failed to provide any suggestion as to how to effectively develop methods of international co-operation.

According to the above treaty, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of

privacy in the electronic communications sector would require "a provider of a publicly available electronic communications service to take appropriate technical and organisational measures to safeguard the security of its services."

The obligations of the Member States to safeguard their security should be extended beyond the electronic communications sector, as disruption of the enabling information society services would, in turn, prevent the other information society services which rely on them for data and other inputs. Private networks and systems managed by internet staff, or the security of which has been outsourced, should also be closely monitored. Disproportionate financial and administrative burdens on small operators and users should be avoided.

8. CYBERCRIME AND INTERNATIONAL LAW

Methods of hacking confidential information by technological means or otherwise (the latter by "individuals") amount to intervening in the usual course of affairs of the victim state, in addition to making it vulnerable to further attacks. Thus, hacking from foreign jurisdictions is a form of attack on the security of a state by force, which act should come under the purview of Article 2, paragraph 4 of the UN Charter. Much has already been published on the legal aspects of the use of force and "intervention" – for further information see for example A D'Amato, "The Invasion of Panama was a Lawful Response to Tyranny", 84 *American Journal of International Law* (1990) 516; L Henkin, "The Invasion of Panama under International Law", 29 Columbia Journal of Transnational Law (1991) 293; and C Gray, *International Law and the Use of Force,* Oxford, Oxford University (2000). Suffice to say that it is a novel kind of intervention, the ulterior motive of which is far-reaching and devastating ranging from say, destruction of infrastructure in a country, to de-stabilising her political system.

On the grounds of the protective principle or the universality principle, a victim state may assume jurisdiction in defiance of the "location" theory, provided of course, the perpetrator of the crime has been found. If however, cybercrime is committed by a state or a state institution, then the problem of tracing the perpetrator would not arise. In the latter situation however, the accused (the state or the state institution concerned) may rigidly adhere to the location theory, and succeed before the courts of law of the victim state, unless the victim state's judiciary is able to establish that justice may not be done by the judicial system of the foreign jurisdiction. The following may be the sustainable grounds to justify that agreement: the lack of rule of law; lack of evidence; non-availability of appropriate witnesses within that jurisdiction; and that the decision of the court may not be effectively enforced by the courts of the accused.

For a discussion on the location theory, see for example *In re Union Carbide Gas Plant Disaster at Bhopal, India* 809 (USCA 2nd civ) reproduced in 26 *International Legal Material* (1987) 1008. Although it was not a case of transnational crime, but a case which predominantly based on negligent act on the part of a US company, the location theory was applied; P Muchlinski, "The Bhopal Case: Controlling Ultrahazardous Industrial Activities Undertaken by Foreign Investors", (1987) 50 MLR 545.

"Hacking" satisfies the basic elements of a criminal act. It is a transnational offence, but it presents the problem of locating the "offender". This, in turn, presents jurisdictional problems unless one takes the view that the universality principle will apply to cybercrimes. The general principle of jurisdiction in international law in respect of criminal acts was settled by *The Lotus*, judgment No 9 (1927), PCIJ, Series A, No 10; the location of a criminal act determines the jurisdiction – that is, the courts in that jurisdiction will assume jurisdiction. It is also important to bear in mind that where citizens of a state are killed or harmed by others, including external entities, that state under international law must be allowed to prove its innocence or non-involvement in that incident. In *The Lotus* this issue assumed importance, as eight Turkish citizens were killed when the boat sank. The Permanent Court of International Justice allowed Turkey to assume jurisdiction to deal with the issue of liability of the parties to the dispute.

The settlement of cybercrime-related disputes presents another difficulty. The International Criminal Court deals with individual criminals and not states. The International Court of Justice may have authority to assume jurisdiction over such disputes perhaps on the grounds of the Article 2(4) of the UN Charter; see however "Germany v US Request for the Indication of Provisional Measures", Provisional Measures Order issued by the International Court of Justice on 3 March 1999, reproduced in 38 International Legal Materials (1999) 308; and *The Case Concerning Angel Francisco Beard*, Decision of the International Court of Justice reproduced in 37 *International Legal Materials* (1988) 810.

Thus, given the current institutional structure of settling this type of disputes, the other alternatives would be to refer them either to the relevant domestic law courts or to ad hoc tribunals, bearing in mind that the awards rendered by the latter institutions may not be enforced at all by the party against which they have been handed down.

On the other hand, the location of crime theory is deep-rooted in legal systems because the location of the crime should be regarded as the most appropriate jurisdiction for dealing with transnational crimes. However, with the perpetrators of cybercrimes being located in a variety of jurisdictions, no particular jurisdiction may be accorded any priority over the other where cybercrimes are committed in concert. However, by relying on the principle of state responsibility and the notion of national security there may be a strong argument to support the view that the location of consummation of crime, where the effect of it has become so manifest, should

ideally be the location for rendering a judgment. It is quite possible that the place of initiation of crime and the location of its consummation coincide, but where they do not do so the place of consummation of crimes may be the most appropriate jurisdiction to render judgment a on them.

It can also be said that departures from the location theory have become a common phenomenon, usually on the grounds of the national interest. Those states which follow a dualist doctrine will only accept international obligations through the process of incorporation of their treaty obligations into their national legal systems. Most states are dualists; when "national interests" form the basis for assuming jurisdiction, and the sovereign state concerned would not really be amenable to any other jurisdiction, assumption of jurisdiction in respect of a transnational crime by the courts in the state in which harm has been caused and suffered would be allowed as that court would be the natural forum.

On the basis of "effect doctrine", the courts of the state the security of which has been endangered or jeopardised – or if its citizens have been adversely affected as a result thereof, or both – may be allowed to assume jurisdiction. In English law, where a murder or manslaughter is committed by a British citizen outside of its jurisdiction, under section 9 of the Offences against the Person Act 1861 and section 3 of the British Nationality Act 1948, English courts may assume jurisdiction over that offence, and the authority of the court does not seem to be subject to any limitation of time (see *R v Cheong* [2006] All ER (D) 385).

There are two main theories to justify the exercise of the national jurisdiction when a crime originates abroad: (a) the protection theory, which has already been briefly discussed; and (b) the objective territoriality theory. According to this latter theory, particularly in relation to cybercrimes, the victims are usually the states; the harm is caused to the states, and any theoretical approach to defy the claim of the affected states would be unreasonable and unacceptable. Crime is effectuated in the victim state, and this establishes the connection. This situation also overlaps with the theory of the national interest. . Conversely, if a British citizen commits a crime whilst abroad against Britain, that citizen shall be tried by the English courts. The celebrated case on this point is *Joyce v DPP* [1946] AC 347.

The US practice on the issue of assumption of jurisdiction by the US courts where crimes are committed abroad, whether by its own citizens or aliens, is clear. Based on the "harm" theory the US courts shall assume jurisdiction. Currently, the cases of Edward Snowden and Julian Assange are in point. Even though both of them are currently living in overseas jurisdictions, it may be assumed that upon their entry on the US soil, they will be arrested and tried in the US.

The US Commercial Code asserts a number of items which would come under the purview of the special maritime and territorial jurisdiction of the United States, for example:

- the high seas and any other waters within the admiralty and maritime jurisdiction of the US and one of the jurisdictions of any particular state, including any vessels owned by US individuals who are travelling on them;
- any vessel travelling on the Great Lakes connecting waters or the St Lawrence River, where it forms point of Canada and the US border;
- any US aircraft having a scheduled departure from or arrival in the US in regard to an offence committed by or against a national of the US; and
- offences committed by or against a national of the US in diplomatic missions, consulates and military posts outside of the US.

This is not the end of the list; there also exist a number of Acts authorising US courts to assume jurisdiction for acts done by or against US nationals outside of the US but having effect on the US. The decided cases on this issue are innumerable. The Military Extraterritorial Jurisdiction Act (MEJA) is another example of US authority to assume jurisdiction for acts committed outside of the US.

Enforcement of judicial orders, whether by the UK or the US, may present difficulties unless:

(a) the accused voluntarily surrenders to the US jurisdiction;

(b) there exist bi-lateral mutual assistance treaties between these countries and the other countries concerned; or

(c) there exists a truly international treaty to which a large number of the members of the international community are parties, and they have accepted the obligation to enforce that treaty, which in the contemporary world is highly unlikely.

9. THE ROLE OF DIPLOMACY IN OVERCOMING CYBER SECURITY-RELATED PROBLEMS

It has already been pointed out that cybercrimes may not be effectively dealt with by technology. One should go into the causes of animosities between states. It would be inappropriate to go into these issues in detail in the context of this article; suffice to point out however that the only effective means of resolving world problems would be by diplomatic means, and not by weapons or technology or by law alone. Thus, a new form of diplomatic negotiating skills would be essential to convince the international community that a novel avenue for peace-making must be created, bearing in mind that it is easier to destroy things than create them. States must appreciate that the days of power-based diplomacy are over; the days of espionage leading to cybercrimes should be over too. However, emotional it may sound, aggressive diplomacy will not do anymore. A new customary law should be developed by

means of a binding convention along the lines of the Nuclear Test Ban Treaty, which should be urgently brought into force and include in it cybercrimes as an international crime. Then comes the issue of "international co-operation" which is a "buzz" word in international relations and international law. Most of the international conventions, as a matter of practice, include this term, but one should critically consider the effect of it in reality.

10. CONCLUSIONS

International co-operation is a term which one often comes across in reading literature on public international law, international relations and international institutions. This term has been incorporated into almost every resolution or recommendation adopted by the UN General Assembly or the Economic and Social Council. But what is it? How many examples of international co-operation exist, in reality, to exemplify it? There are two apparent reasons for the lack of international co-operation: (a) how sovereign states perceive the concept of sovereignty; the sharing of functional sovereignty is essential for developing co-operation among sovereign states; and (b) sovereign states often fail to appreciate the benefits that they may derive through interaction with other sovereign states.

According to the *Oxford Dictionary of English* (3rd ed, 2010) the term "co-operation" means "… the action or process of working together to the same end." The essential pre-requisites for international co-operation would be: (a) to have a "mind-set" for working together; in order to be able to do that (b) sovereign states should appreciate that they will be required to use what may be described as the "functional" sovereignty which does not impact their politico-legal sovereignty; (c) an understanding on the part of the sovereign states of the importance of working together to deal with international issues and matters; and (d) also a genuine understanding of the importance of working together at international fora on common issues which adversely affect the entire international community, and that no one state, however powerful it might be – economically militarily or otherwise – may eradicate certain problems.

Returning to the concept of "functional sovereignty", it is worth referring to *Territorial Jurisdiction of the International Commission of the River Oder* PCIJ (1929) Series A, No 23. In that case the Polish contention was that under the Treaty of Versailles, the jurisdiction of the International Commission of the Oder did not extend to the tributaries of the Oder, Warthe and Netze, which were situated in the Polish territory. By nine votes to three, the Permanent Court of International Justice held that the Commission's jurisdiction did so extend under Article 331 of the Treaty. The court drew analogies with the position of the rivers Elbe and Niemen; indeed Article 331 of the Treaty also included the River Oder.

In deciding on the matter, the court mentioned, *inter alia,* certain important terms, which upon analysis, would hint what may be regarded as some of the essentials of international co-operation: "community of interest", "common legal right" and "internationalisation of a river". In order to achieve international co-operation over any issue, internationalisation of the issue would be a prerequisite, and apart from anything else, a "community of interest" must also be perceived by the international community. These would be the manifestation of functional sovereignty.

Doran maintained in, *inter alia*, in "The Two Sides of Multilateral Co-operation" that a greater sense of threat affecting states might trigger co-operation among them: see I W Zartman and S Touval (eds), *International Co-operation: The Extent and Limits of Multilateralism,* Cambridge, Cambridge University Press (2010) at 40. He emphasised that it is the act of competition with the aggressor that causes the other governments to co-operate among themselves. Although such a view may be supported by historical examples (Napoleon's defeat by the United Europe) it may be difficult to sustain this view in the contemporary period for two main reasons: (a) under Article 2(4) of the UN Charter any act of "aggression" by a Member State against another is prohibited; and (b) states are not supposed to co-operate against an aggressor state. Certain obstacles to developing international co-operation would be difficult to overcome – financial or economic (trade) or military dependence on some other states, or even a policy of "indifference" to becoming involved in matters of "international concern", or the lack of understanding of the "functional aspect" of sovereignty which is a sine qua non for developing a "community of interests". Thus, cybercrimes which need international co-operation for solution, rather than counter-cyberattacks, may continue in an unabated fashion.

In their joint work *Introduction: Return to the Theories of Co-operation,* Zartman and Touval maintained that there may not be any co-operation without conflict. According to them, "… attempt of co-operation may create conflict … since the parties' attempt to work together brings out differing interests to be tailored to fit the costs of co-operation." Conflicts, they maintain, stand for perception of incompatibilities. It would be unfortunate to apply this condition to achieving international co-operation in the sphere of international law, one of the principal objectives of which is established in the UN Charter, that is, to achieve its purposes by peaceful means. No co-operation between states may be achieved unless they voluntarily subjugate themselves to international instruments; namely, international conventions, Declarations or Resolutions adopted by the United Nations, or even those of non-governmental bodies such as the International Red Cross. *Pacta sunt servanda* is a sacrosanct principle of all agreements both at national and international levels. At an international level, however, treaties must be respected, and the distinctions between treaties and conventions or charters are often blurred (see also Grotius, *De Jure Belli ac Pacis* (1625); chapter 19 of Book 3 bearing the title of *De fide inter hostes*

refers to the sanctity of agreements even between enemies: *fides et hosti servanda* etc). The Treaty of Westphalia, the Nuclear Test Ban Treaty or the UN Charter or the Vienna Convention on the Law of the Sea or the UN Convention on the Law of Treaties (UNCLOS III) are all based on the principle of *pacta sunt servanda*, but unfortunately the reality has proved to be different – particularly in respect of the UN Charter.

Good faith is the central theme of the sanctity of agreements between states; when these instruments are not respected by the signatories, then the obvious conclusion would be that they did not accept them in good faith. In his work *De Jure Belli* ac Pacis, Grotius considered *fides* as the basis of justice, which concept was related to treaties by Bodin even before the time of Grotius (1576, Book V, Ch 16; see also R Kolb, *La Boane foi et droit international public,* Paris, Presses Universitaines de France (2000)). Whereas Grotius very optimistically maintained that the international community would be responsible for enforcing agreements – being convinced that although man is an animal, he is an animal of a superior kind – Hobbes in *Leviathan* (1651) clearly maintained a diametrically opposite view. The state of nature is not friendly; it is one of perpetual wars between the participants in it. No wonder Hobbes also maintained that anarchy directs international relations; thus morality and "justice" seem to be irrelevant concepts to states. To break out of that attitude would be a difficult task for states to achieve.

On the other hand, Pufendorf believed in "sociability" as the keystone for all states, which unfortunately does not seem to be the state practice at least in the contemporary period of time. States' real interests have been to reign supreme – perhaps that is one of the principal reasons for the revocation of obligations emanating from international instruments. Again, Locke's state of nature is untenable; it oscillates between war and peace. Thus, briefly, Grotius's theory tends to prevail. Otherwise, it is unfortunate that despite a new vow after the Second World War to establish "peace" through the UN, the international community has failed its objectives.

The above discussion may make the reader depressed, but unfortunately, the conduct of the international community in dealing with matters of international concern has prompted the authors to lay the history of international co-operation bare. Nevertheless, within a pessimistic scenario one can still identify some rays of hope, and hope in this context should be made a reality by and through diplomats. The traditional perception of developing power-based international relations should be reviewed. In terms of technological might, there will remain significant gaps between developing countries, in general, and the rich countries and emerging markets for the foreseeable future.

Dr Charles Chatterjee

LLM (Cambridge), LLM, PhD (London), Barrister; Associate Research Fellow, IALS

Anna Lefcovitch

LLM, Solicitor, Arcadis LLP

The opinions expressed in this article are those of the authors, and in no way may be attributed to the institutions with which the authors are affiliated.