

Note from the Executive Board

Dear Delegates

It is with distinct pleasure that we welcome all of you to this exciting simulation of the International Multilateral Partnership Against Cyber Threats (IMPACT) at Nanyang Technological University Model United Nations 2012. It is indeed an honour for us to be chairing this perhaps unconventional committee, and we would like to remind you that this council will be markedly different from others that you may have experienced.

In addition to being diplomats, you will also be expected to exhibit technical understanding and analytical reasoning in your deliberations. This background guide should serve as a reference for your research, however, literature on the topic at hand (cyber-security) is vast, and you may delve as deeply as necessary to come up with a comprehensive and meaningful resolution to the issue at the end of this 3 day conference.

Wishing you the best of luck

Regards

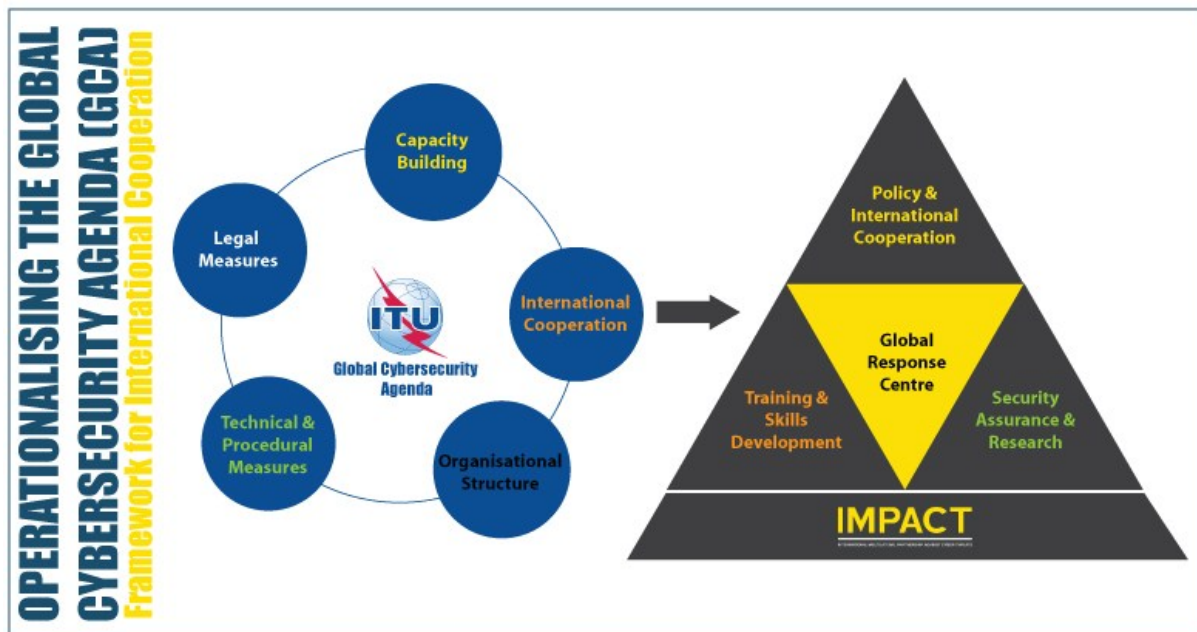
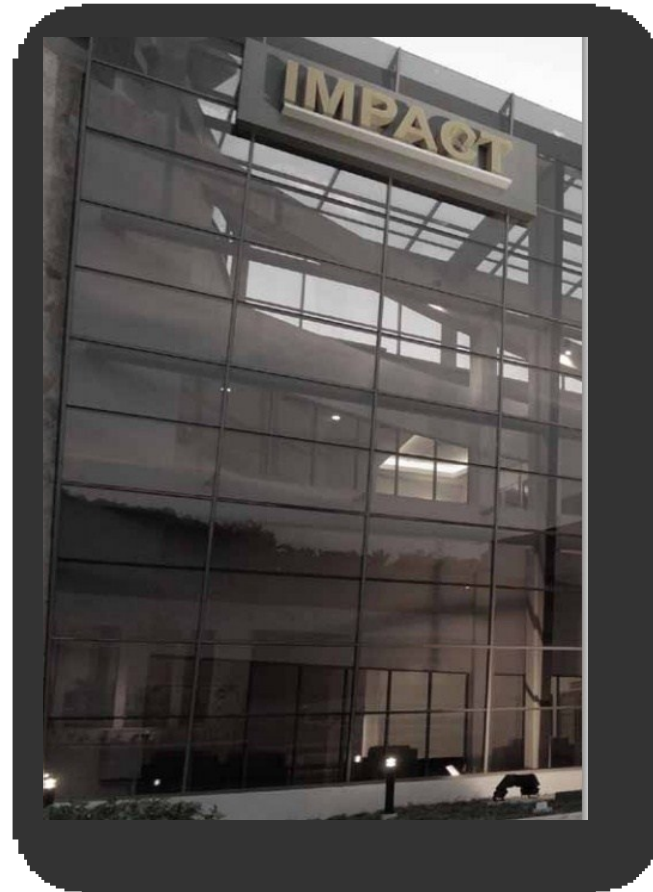
The Executive Board

PS: We understand that this guide comes a tad too late for it to be of substantial help, but do read through it and refer to it during the actual session to allow the IMPACT to work within its mandate and deal with the issues effectively. We've covered the scope in two broad areas – the committee and the issue at hand. Keep these in mind and rest assured that we'll guide you as the committee progresses. ☺

Introduction: What is IMPACT?

The **International Multilateral Partnership Against Cyber Threats (IMPACT)** is a comprehensive global public-private partnership alliance against cyber threats. IMPACT is the cyber-security arm of the United Nations' specialised agency for ICTs, the International Telecommunication Union. As the world's first comprehensive alliance against cyber threats, IMPACT brings together governments, academia and industry experts to enhance the global community's capabilities in dealing with cyber threats.

Based in Cyberjaya, Malaysia, IMPACT is the operational home of ITU's Global Cyber-security Agenda (GCA). IMPACT offers ITU's Member States with access to expertise, facilities and resources to effectively address cyber threats, as well as assisting United Nations agencies in protecting their ICT infrastructures.



Collaboration with the ITU

IMPACT is tasked by ITU with **the responsibility of providing cyber-security assistance** and support to ITU's 193 Member States and also to other organisations within the UN system. The Memorandum of Agreement was officially signed by ITU Secretary-General Dr. Hamadoun Touré and Datuk Mohd Noor Amin, Chairman of IMPACT at the ITU's head office

in Geneva. Founded in 1865, ITU is the oldest organisation within the UN system and functions as the UN's specialised agency for information and communication technologies.

IMPACT's involvement with ITU began in 2008 when it was chosen as the physical home of ITU's Global Cyber-security Agenda (GCA). The GCA is an international cyber-security framework that was formulated following deliberations by more than 100 leading experts worldwide. The GCA contains many recommendations, which when adopted and appropriately implemented, would result in improved cyber-security for the global community of nations. Through a Memorandum of Understanding inked back in 2008, ITU made IMPACT the physical home of the GCA and had tasked IMPACT with the responsibility to operationalize the various initiatives under the GCA.

In addition to this, during the 2011 WSIS Forum, a **Memorandum of Understanding (MoU) was signed between ITU and the United Nations Office on Drugs and Crime (UNODC)** which will see IMPACT playing a pivotal role in supporting both organisations in their collaboration to assist UN member states mitigate risks posed by cybercrime. IMPACT's Global Response Centre (GRC) acts as the foremost cyber threat resource centre for the global community and provides emergency responses to facilitate identification of cyber threats and sharing of resources to assist ITU-UNODC Member States.

Global Support System

The international community, both in the public and private spheres – has given its wide-ranging support to IMPACT from its inception.

- The Malaysian Government provided US \$13m in seed funding with a view to establish IMPACT's central headquarters equipped with the best facilities for international community.
- [F-Secure](#) has contributed its expertise in establishing IMPACT's Global Response Centre – designed as the first line of defence against cyber threats.
- [Kaspersky Lab](#) provided technical expertise in setting up IMPACT's Network Early Warning System (NEWS) in the Global Response Centre.
- [SANS Institute](#) and [EC-Council](#) has contributed a grant of US\$1m each to IMPACT to create scholarships schemes for developing nations that will help enhance and build capacity and capability in cyber-security.
- [Symantec Corporation](#) assisted by establishing a Centre of Excellence for IMPACT's Government Security Scorecard.

IMPACT Services



Global Response Center

Working with leading partners from academia, governments and industry (current partners include Symantec Corporation, Kaspersky Lab, F-Secure, Trend Micro, Microsoft and many other stakeholders), the GRC provides the global community with a near real-time aggregated early warning system. The GRC's 'Network Early Warning System' (NEWS) helps partner

countries identify cyber threats on the onset and provides critical guidance on what measures to take.

The GRC provides the ITU's Member States with access to specialised tools and systems, including NEWS and 'Electronically Secure Collaborative Application Platform for Experts'

Key Features of the GRC:

- Network Early Warning System
- Expert locator
- Team Management
- Remediation facility
- Automated Threat Analysis System (ATAS)
- Trend libraries
- Global visualization of threats
- Country specific cyber threats
- Incident and case management
- Trend monitoring and analysis
- Knowledge base
- Reporting
- **IMPACT Honeynet**

NEWS

NEWS is a platform of collaborative mashup of information from multiple early warning alliances and cyber-security vendors. This aims to get the right information to the relevant authorities in a timely manner, enabling them to mitigate and effectively respond to cyber threats that may arise from around the world. Working with leading partners from academia, industry, and international bodies, NEWS provides the global cybersecurity community with real time aggregated early warnings. It also manages the access rights, permissions, information security of the data collected and heightens privacy to sensitive information.



the GRC with a tremendous amount of data related to cyber threats, which is disseminated through the NEWS platform thereafter, for remedial in-country action. In addition to the existing providers, GRC – through the NEWS platform – seeks to add more comprehensive data resource providers. With its tremendous amount of cyber threat-related data, NEWS will be the richest knowledge base of its kind in the world.

Current leading industry partners in cyber-security feed tremendous amount of data related to cyber threats, which is disseminated through the

ESCAPE

ESCAPE is a tool that allows cyber-security experts across different countries to pool their resources, share their expertise and remotely collaborate in a secure environment. The ESCAPE platform enables the GRC to act as a one-stop coordination and response centre for countries in times of crisis, enabling the swift identification and sharing of available resources.

Key features

- Knowledge Exchange Network (KEN)
- Automated Threat Analysis System (ATAS)
- Incident Reporting and Response System

Centre for Policy and International Cooperation

IMPACT believes that enforcers and international security organisations, along with governments and the private sector, need to collaborate to find effective solutions given the scope, severity and transnational nature of this problem. Indeed, the governance of cyberspace is fast becoming a major challenge, not only at a national level, but also at a regional and global level.

Clearly, governments cannot contain cyber threats by domestic measures alone. Without expert collaboration and knowledge sharing, individual countries hamper their ability to

respond to cyber threats. No single government possesses all the knowledge and expertise to counter cyber threats. In most cases, the expertise and know-how reside in the private sector and academia. It is therefore imperative that all stakeholders — governments, industry and academia — unify to share the information and resources that will amplify the world's cyber-security expertise.

IMPACT, through its Centre for Policy and International Cooperation, seeks to create a platform by which the various stakeholders can come together and collaborate; escalating the culmination of knowledge and tools that will ensure a safer, more secure cyberspace.

The current focus of the Centre for Policy is the following:

- Promotion of cyber laws and the global harmonisation of national cybercrime legislation
- Awareness raising and mitigation of cyber crime and other forms of cyber threats
- Promotion of child online protection issues and solutions

Centre for Security Assurance and Research

While governments have cyber-security policies as part of their security measures, the enforcement of policy compliance has always been a daunting challenge.

In order to tighten and achieve compliance, a total automated solution, such as the IMPACT Government Security Scorecard (IGSS) is needed.

Through a centralised and automated analysis of a government's critical business applications and infrastructure, authorised personnel can effectively manage risks by identifying weaknesses and measuring compliance with security practices and regulation requirements. Through its reporting capabilities, IGSS enables the government to understand the critical components of its security postures by analysing compliance at a national-level; this can be filtered down to the region or office level. With IGSS, partner countries will have ONE dashboard view of their security posture and position via an automated audit environment.

Other measures include **sharing of threat data, Child Online Protection (COP) and INTERPOL's Internet Access Blocking Initiative.**

Cyber Security: What is it all about?

"One of the most serious economic and national security threats our nation faces."

- Barack Obama on Cyber Security

In the age of modern technology and blazing connectivity across borders through the internet, cyber security is a new threat to today's world. The growing number of attacks on our cyber networks has become rather large and **not only does it span across borders, but also covers different sectors and activities with the new age cyber-terrorism also becoming a rage**. Nations are looking forward to building teams to keep their federal civilian networks secure, and securing the cyberspace and critical infrastructure on which their nations depend, much like how the Department of Homeland Affairs supports the USA in dealing with cyber threats.

While governments need to have their own systems in place to deal with immediate threats, there is a greater importance to deal with private companies and organizations who specialize in this sector, **and this is where IMPACT comes into play**. As a committee it serves to address these issues in specific with organizations which are capable of handling them, such as Symantec, but under the aegis of the United Nations, it serves to bring nations together and effectively mediate these issues on a global scale.

Parties involved

Certain nations like **The People's Republic of China and Israel** have hackers under their intelligence, while a number of private groups like **Chaos Computer Club** choose to manifest themselves in either a nation, or a group of nations with commonality, in this case the language German. There are also groups like **Lulzsec and Anonymous** which regularly take down websites through use of Denial of Service attacks, phishing hacks as well as server side attacks. However, the intended purpose of that attack remains undefined – while groups choose to carry out attacks to raise an issue, much like what Anonymous recently carried out in protest of **Stop Online Piracy Act (SOPA)**, there have been attacks carried out by nations (or coalitions) against other nations in the world. The **Stuxnet** worm, used to infect Iranian Nuclear Enrichment Plants, attacked the Programmable Logic Controllers and could have **possibly led to disastrous consequences at the Nuclear facilities at Natanz** in Iran and while the nature of attack was understood, it is still unknown as to who exactly carried out the attacks, and whether any nation-support existed in the facilitation of the act itself, with **much suspicion towards the United States of America and the Israeli Defence Forces**. This, however, remains an incomplete list with many other actors and parties out there.

Recent Incidents

Computer Virus hits US Predator and Reaper drone fleet (November 2011)

A computer virus had **infected the cockpits of America's Predator and Reaper drones, logging pilots' every keystroke as they remotely flew missions over Afghanistan and other war zones.**

The virus, first detected by the military's Host-Based Security System, had not prevented pilots at Creech Air Force Base in Nevada from flying their missions overseas. Nor had there been any confirmed incidents of classified information being lost or sent to an outside source. **But the virus had resisted multiple efforts to remove it from Creech's computers, network security specialists say.** And the infection underscores the on-going security risks in what has become the US military's most important weapons system.

"We kept wiping it off, and it kept coming back," said a source familiar with the network infection, one of three that told Danger Room about the virus. "We thought it's benign. But we just don't know."

Military network security specialists aren't sure whether the virus and its so-called "keylogger" payload were **introduced intentionally or by accident**; it may be a common piece of malware that just happened to make its way into these sensitive networks. The specialists **don't know exactly how far the virus has spread.** But they're sure that the infection has **hit both classified and unclassified machines at Creech.** That raises the possibility, at least, that secret data may have been captured by the keylogger, and then transmitted over the public internet to someone outside the military chain of command.

[The possibility of drones being taken into control and used to achieve purposes for other nations or terrorist groups in the name of the USA would mean both sectors of terrorism and cyber security are compromised. Issues here would deal with the nature of cyber terrorism and what it stands for both, in this context and in and of itself.]

New JavaScript hacking tool can intercept PayPal, other secure sessions (November 2011)

A pair of security researchers presented a hacking tool which decrypted secure Web requests to sites using the Transport Layer Security 1.0 protocol and SSL 3.0, allowing a person or program to hijack sessions with financial websites and other services. Juliano Rizzo and Thai Duong unveiled their Browser Exploit Against SSL/TLS tool, dubbed BEAST, at the Ekoparty security conference in Buenos Aires.

The tool is based on a blockwise-adaptive chosen-plaintext attack, a man-in-the-middle approach that injects segments of plain text sent by the target's browser into the encrypted request stream to determine the shared key. The code can be injected into the user's browser through JavaScript associated with a malicious advertisement distributed through a Web ad service or an IFRAME in a linkjacked site, ad, or other scripted elements on a webpage.

Using the known text blocks, BEAST can then use information collected to decrypt the target's AES-encrypted requests, including encrypted cookies, and then hijack the no-longer secure connection. That decryption happens slowly, however; BEAST currently needs sessions of at least a half-hour to break cookies using keys over 1,000 characters long.

The attack, according to Duong, is capable of intercepting sessions with PayPal and other services that still use TLS 1.0—which would be most secure sites, since follow-on versions of TLS aren't yet supported in most browsers or Web server implementations.

While Rizzo and Duong believe BEAST is the first attack against SSL 3.0 that decrypts HTTPS requests, the vulnerability that BEAST exploits is well-known; BT chief security technology officer Bruce Schneier and UC Berkeley's David Wagner pointed out in a 1999 analysis of SSL 3.0 that "SSL will provide a lot of known plain-text to the eavesdropper, but there seems to be no better alternative." And TLS's vulnerability to man-in-the middle attacks was made public in 2009. The IETF's TLS Working Group published a fix for the problem, but the fix is unsupported by SSL.

[Two issues here – first being that of the nature of online security and whether that needs greater enforcement and secondly, the possibility of a compromise of secure information for those who use the popular site PayPal for their online transactions, which requires personal details including credit card numbers.]

Anonymous downs government, music industry sites in largest attack ever (January 2012)

Hactivists with the collective Anonymous are waging an attack on the website for the White House after successfully breaking the sites for the FBI, Department of Justice, Universal Music Group, RIAA and Motion Picture Association of America.

In response to today's federal raid on the file sharing service Megaupload, hackers with the online collective Anonymous have broken the websites for the FBI, Department of Justice, Universal Music Group, RIAA, Motion Picture Association of America and Warner Music Group.

"It was in retaliation for Megaupload, as was the concurrent attack on Justice.org," Anonymous operative Barrett Brown tells RT on Thursday afternoon.

Only hours before the DoJ and Universal sites went down, news broke that Megaupload, a massive file sharing site with a reported 50 million daily users, was taken down by federal agents. Four people linked to Megaupload were arrested in New Zealand and an international crackdown led agents to serving at least 20 search warrants across the globe.

Less than an hour after the DoJ and Universal sites came down, the website for the RIAA, or Recording Industry Association of America, went offline as well. Shortly before 6 p.m EST, the government's Copyright.gov site went down as well. Thirty minutes later came the site for BMI, or Broadcast Music, Inc, the licensing organization that represents some of the biggest names in music.

Also on Thursday, MPAA.org returned an error as Anonymous hackers managed to bring down the website for the Motion Picture Association of America. The group, headed by former senator Chris Dodd, is an adamant supporter of both PIPA and SOPA legislation. Universal Music Group, or UMG, is the largest record company in the United States and under its umbrella are the labels Interscope-Geffen-A&M, the Island Def Jam Motown Music Group and Mercury Records.

Brown adds that “more is coming” and Anonymous-aligned hackers are pursuing a joint effort with others to “damage campaign raising abilities of remaining Democrats who support SOPA.” Although many members of Congress have just this week changed their stance on the controversial Stop Online Piracy Act, or SOPA, the raid on Megaupload Thursday proved that the feds don’t need SOPA or its sister legislation, PIPA, in order to pose a threat to the Web. Brown adds that operatives involved in the project will use an “experimental campaign” and search engine optimization techniques “whereby to forever saddle some of these congressmen with their record on this issue.”

[This really exposes the impact which private groups like Anonymous can have, and more so in the current context where DoS attacks are launched through mass mobilization and the use of anonymous Internet Relay Chats]

What to expect as part of a resolution?

Cyber security is a relatively new issue in today's world, and thus there haven't been any global treaties or conventions that underline the responsibilities and actions that must be taken to deal with security breaches and threats globally. We'll analyse this through heuristic questions:

What is cyber security?

While there is a definition to what it literally means i.e. protection of information and property from theft or corruption while allowing it to be used by the intended users, there is no definition on what it really encompasses. Delegates need to explore the various facets under the ambit of cyber security and analyse the potential impacts of security lapses under these themes. Issues like 'cyber terrorism' would help define key terms effectively – what constitutes a crime, how prosecution would be carried out – based on cyber actions alone or whether the act of insinuation also constitutes a crime, and under what law will these 'terrorists' or perpetrators be judged, especially with the global nature of cyber warfare.

Who are the actors?

Essentially, dealing with nations as well as private actors would be necessary, since a different set of laws would apply to both. Other actors and middle-players could also be considered in the larger scope of this issue.

Where is the area of conflict?

Delegates need to address the kinds of acts that are taking place – firstly, that of state sponsored cyber warfare and security breaches, secondly, acts carried out by individuals as to send a message or use scare tactics, and lastly the new age means of activism, 'hactivism', which has formed 'organized cyber threats' under various groups like Lulzsec and Anonymous.

When and how do we act?

Delegates need to realize the nature of cyber action and the immediacy of the impacts that it has. Thus, delegates are advised to look into various time frames suitable to the issues as they come up. Reaction mechanisms are a core of IMPACT and thus need to be a part of this resolution. Some questions to consider would be 'what constitutes an attack', national systems in place, international cooperation between public and private bodies as well as sharing of threat data and developing further infrastructure for regional and international co-operation.