ITU

IMPACT

INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER THREATS

IMPACT AT A GLANCE

The International Multilateral Partnership Against Cyber Threats (IMPACT) is the cybersecurity executing arm of the United Nations' specialised agency for ICTs, the International Telecommunication Union (ITU). 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 Cybersecurity 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.

IMPACT SERVICES OVERVIEW

ITU-IMPACT's Global Response Centre (GRC) is designed to be the foremost resource centre for cyber threats in the world. Working with leading partners from academia, governments and industry such as Symantec Corporation, Kaspersky Lab, F-Secure, Trend Micro, Microsoft and ABI Research, the GRC provides the global community with a near real time aggregated early warning system for cyber threats.

As partners of ITU-IMPACT, countries have free access to the GRC's specialised tools and systems such as NEWS and ESCAPE to help them combat new and evolving cyber threats.

TECHNICAL

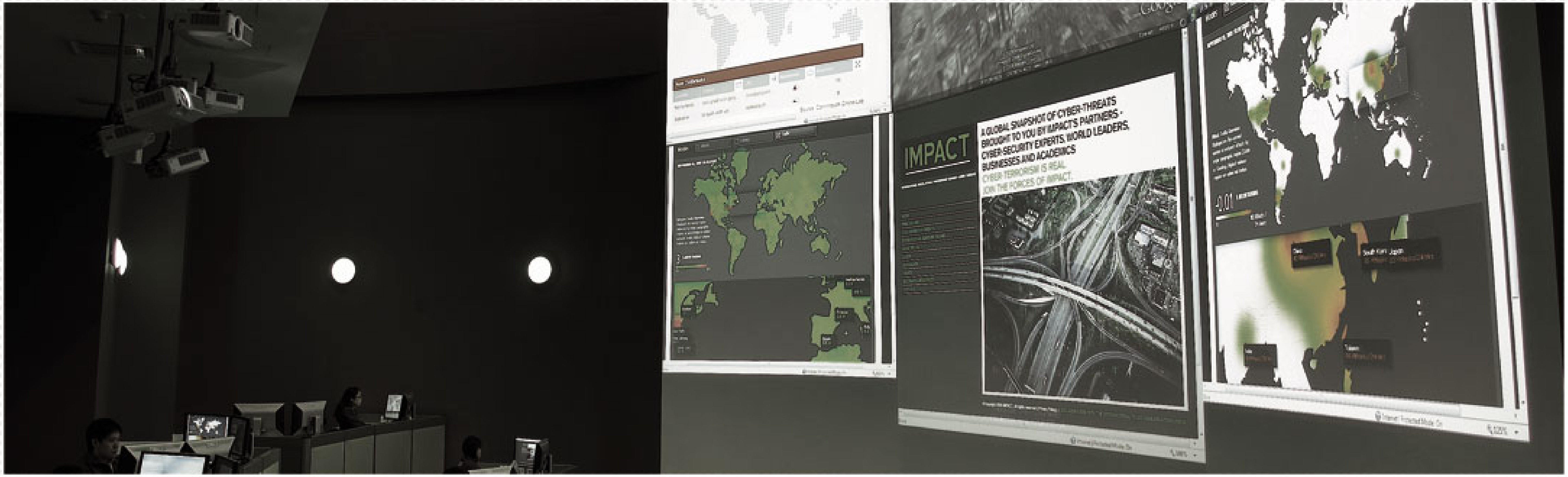
- Network Early Warning System (NEWS)
- Electronically Secured Collaborative Application Platform for Experts (ESCAPE)
- IMPACT Government Security Scorecard (IGSS)
- Computer Incident Response Team (CIRT)
- Vulnerability & web assessment
- Penetration testing

NON-TECHNICAL

- Advisory services on policy and regulatory to partner countries
- Partner country coordination
- Partner management (industry, academia, international organisations)
- Child Online Protection (COP)

CAPACITY BUILDING

- Partner country cybersecurity assessment
- Training
- Workshops
- Seminars
- High level briefings
- Applied Learning For Emergency Response Teams (ALERT)

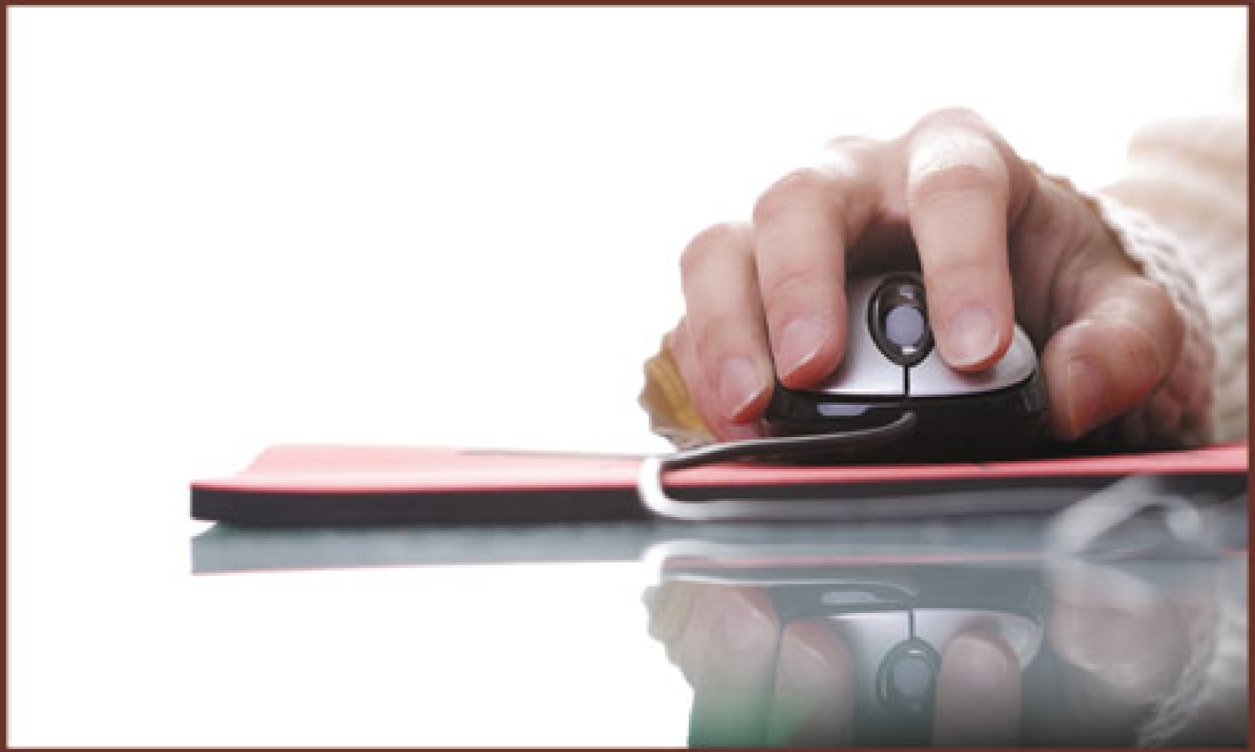

IMPACT
A GLOBAL SNAPSHOT OF CYBER-THREATS BROUGHT TO YOU BY IMPACT'S PARTNERS - CYBER-SECURITY EXPERTS, WORLD LEADERS, BUSINESSES AND ACADEMICS
CYBER TERRORISM IS REAL.
JOIN THE FORCES OF IMPACT.

NETWORK EARLY WARNING SYSTEM (NEWS)

NEWS is a platform of collaborative mash up of information from multiple early warning alliances and cybersecurity 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.

Electronically Secure Collaborative Application Platform for Experts (ESCAPE)

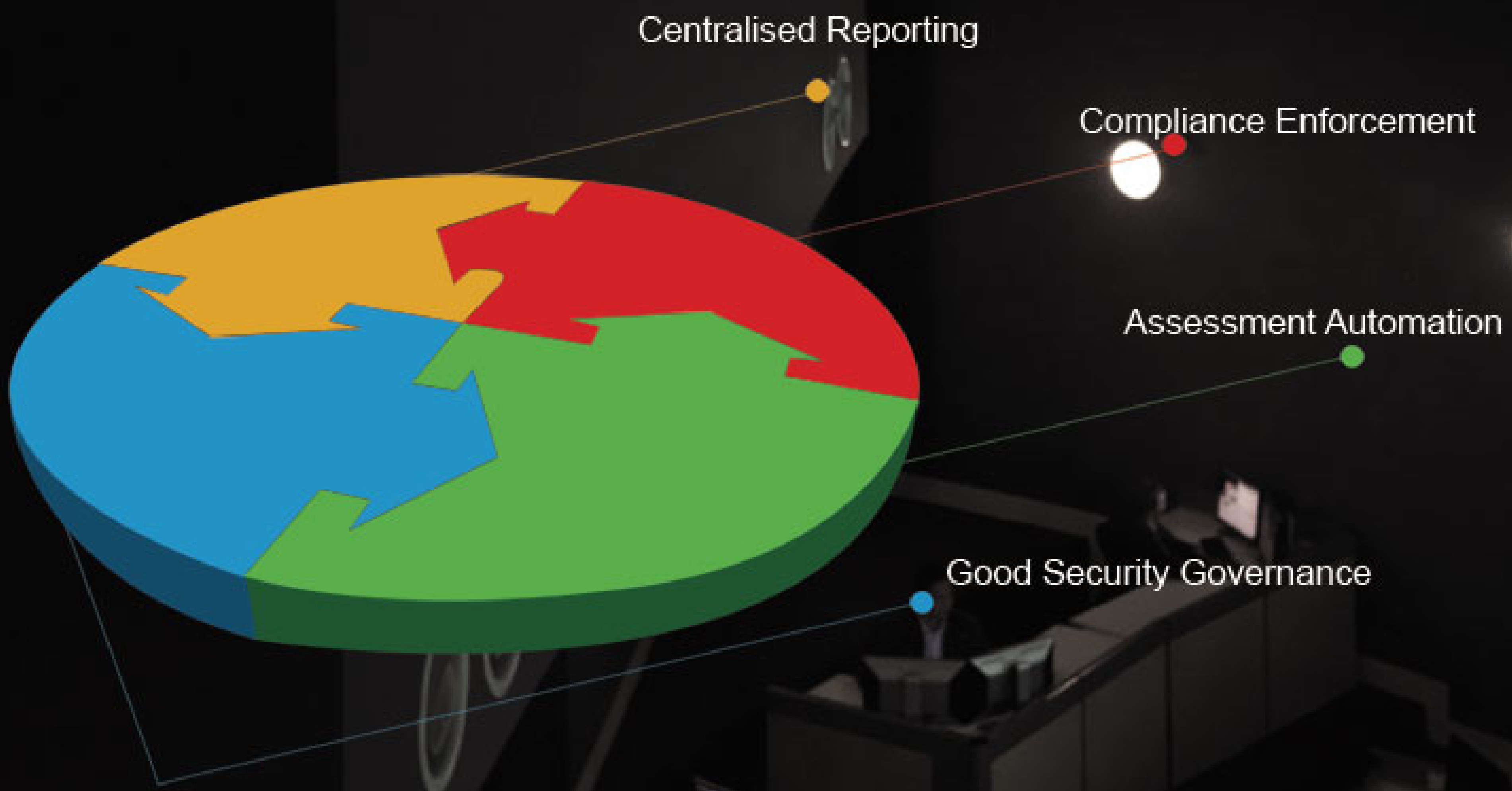
ESCAPE is a tool that allows cybersecurity experts across different countries to pool their resources, share their expertise and remotely collaborate in a secure environment. The ESCAPE platform enables the GRC to act as a one-stop coordination and response centre for countries in times of crisis, enabling the swift identification and sharing of available resources. ESCAPE escalates the speed with which ITU-IMPACT is able to respond to cyber threats, enabling it to draw from a great pool of talent from across numerous locations.



ESCAPE is based on a comprehensive and growing database of key resources around the world which includes IT experts from industry, authorised national-level personnel such as regulators and other trusted parties that can be called upon in times of need. It provides all the tools and solutions needed to ensure that these individuals and institutions are able to collaborate remotely, securely, and effectively.

ITU - IMPACT Government Security Scorecard (IGSS)

IGSS CAPABILITIES



Centralised Reporting

Compliance Enforcement

Assessment Automation

Good Security Governance

BENEFITS OF IGSS

The IGSS helps governments effectively manage risks through a centralised automated system that identifies weaknesses as well as measures compliance with multiple external and internal security regulation requirements. Through its reporting capabilities, IGSS enables governments to understand critical components of their security postures by analysing compliance at a national level which can be filtered down to the regional level.

Benefits of an IGSS Implementation:

A fully automated system of test controls on a scheduled basis enforces compliance to ensure security and prevent data and information losses.

The IGSS ensures real time detection of security control failures as well as security breaches.

A single comprehensive dashboard enables a full view of the security posture and position through the automated audit environment.

A strong reporting capability that provides proof to auditors that IT security policies and regulations are in place and effectively complied.

Computer Incident Response Team (CIRT)

Similar to how a government protects its critical infrastructure from physical threats, it has now become increasingly important to also protect it from cyber threats. Governments across the world have started to realise that a national approach is needed to combat the growth in cyber threats and the CIRT has become an integral part in several national cybersecurity frameworks.

A CIRT assists partner countries in preventing and handling cyber threats by acting as a single point of contact for reporting security incidents as well as providing a platform for information sharing. The CIRT enables monitoring of threats and trends that assist governments in the development of mitigation and response strategies to combat cyber threats.

ITU-IMPACT assists partner countries with CIRT services in three ways:

Capability assessment

Readiness assessment

CIRT implementation

CIRT Capability Assessment

ITU-IMPACT assists the partner country by assessing the capacity and readiness of the national CIRT in identifying, responding and managing cyber threats.

The main objective is to study and evaluate the partner country CIRT's structure and capability to ensure that cybersecurity incidents, intrusion attempts, and emergencies are appropriately managed to levels consistent with industry standards and good business practices.

CIRT Readiness Assessment

ITU-IMPACT can also assist partner countries in the assessment of its readiness to implement a full-fledged CIRT.

The main objectives are to:

- Study and analyse the partner country's current cybersecurity status and needs.
- Provide high level recommendations to improve the cybersecurity posture of the partner country.
- Study and suggest institutional and organisational requirements and arrangements for establishing a national CIRT.

National CIRT Implementation

If a partner country is ready for a national CIRT, ITU-IMPACT can assist and lead the implementation process with the main objectives of:

- Creating and implementing a fully functioning national CIRT to provide its constituents with a basic set of services.
- To implement, review and test day-to-day operations on processes and workflow developed for the CIRT.
- Engage in CIRT capacity building programmes and train at least three government officials from the partner country on CIRT operation and incident response.

Vulnerability Assessment

ITU-IMPACT offers both internal and external vulnerability assessments for partner countries in order to efficiently detect security vulnerabilities and ensure their prompt rectification. This assessment helps partner countries to detect security vulnerabilities across the entire infrastructure before they are breached or exploited by attackers.

Key benefits of this assessment include identification of vulnerabilities before potential attacks, help to mitigate damage to infrastructure and data loss, assistance in budgeting and planning to remediate or mitigate identified vulnerabilities, and ensuring compliance with applicable information security laws, mandates and regulations.

Penetration Testing

Penetration testing is the practice of testing a computer system or network to find vulnerabilities that an attacker could exploit. IMPACT provides its clients with two types of penetration testing; internal and external. External penetration testing focuses on identifying and validating vulnerabilities that exist on all Internet-accessible services within an organisation’s critical IT infrastructure such as web server, email server, DNS, etc. As for the internal penetration testing, it is a comprehensive security test of all systems related directly and indirectly to a business. It mimics the actions of an actual attacker exploiting weaknesses in network security without the usual danger. The test examines internal IT systems for any weakness that could be used to disrupt the confidentiality, availability, or integrity of the network, thereby allowing the organisation to address each weakness.

Web Application Assessment

Web application penetration testing refers to a set of services used to detect various security issues with web applications to identify known vulnerabilities. The test will cover any web application that is accessible over a network like the Internet or an intranet.

The main objectives of the assessment are:

- To discover vulnerabilities in web application interfaces from an external party browser point of view.
- To provide remediation or mitigation of the identified risks, threats and vulnerabilities.

On-Demand Web Application Scanning

The on-demand web application scan is the most accurate and cost effective approach to vulnerability scanning. This proactive on-demand service is cost effective as it eliminates the need for on-premise software solutions and detects vulnerabilities before they are exploited.

The main objectives of the on-demand scan are:

To identify weaknesses and potential vulnerabilities in the partner country's ICT infrastructure in order to determine how secure the system is from theft or damage due to unpatched, weak, or misconfigured security settings.

To proactively address security gaps so that vulnerabilities are promptly rectified before they are exploited.

Child Online Protection (COP)

The Child Online Protection (COP) Initiative was launched by the ITU in November 2008 and aims to bring together partners from all sectors of the global community to ensure a safe and secure online experience for children everywhere.

The COP aims to tackle cybersecurity holistically by addressing legal, technical, organisational, and procedural issues as well as further capacity building and international cooperation.

ITU-IMPACT together with its COP partners has built one of the world's largest repositories for child online protection. The repository includes awareness materials, teaching supplements, videos and tools for parents, educators, industry, and children for partner countries to utilise in creating a safer and more secure online environment for children.

The COP resources are made available to partner countries at no cost and ITU-IMPACT strongly encourages all partner countries to become active participants in the COP framework to ensure a safe cyber environment for children worldwide.

The 5 Pillars and Goals of the COP Global Initiative

Legal measures: Develop national roadmaps and legislative toolkits to help partner countries achieve their COP goals while simultaneously harmonising legal frameworks.

Technical & procedural measures: Develop industry codes of conduct and related technical measures to combat new and emerging threats to children.

Organisational structures: Establish national COP centres, including national hotlines, with multi-stakeholder participation.

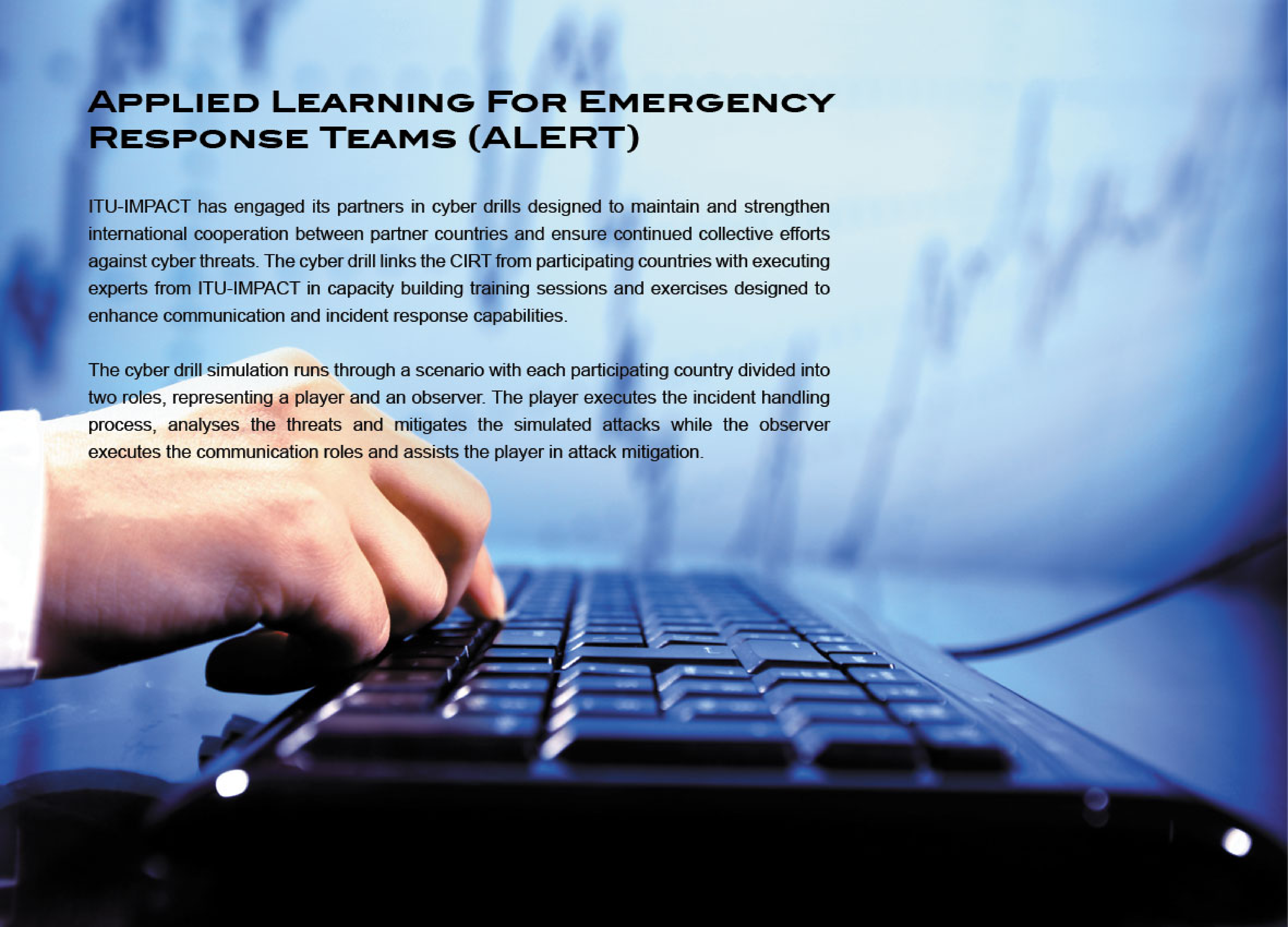
Capacity building: Build human and institutional cybersecurity capabilities, including awareness - raising campaigns, community forums, and training for parents, guardians, educators and children.

International cooperation: Harness the power of a multi-stakeholder collaboration through resources such as online platforms for advice and information sharing.

Applied Learning For Emergency Response Teams (ALERT)

ITU-IMPACT has engaged its partners in cyber drills designed to maintain and strengthen international cooperation between partner countries and ensure continued collective efforts against cyber threats. The cyber drill links the CIRT from participating countries with executing experts from ITU-IMPACT in capacity building training sessions and exercises designed to enhance communication and incident response capabilities.

The cyber drill simulation runs through a scenario with each participating country divided into two roles, representing a player and an observer. The player executes the incident handling process, analyses the threats and mitigates the simulated attacks while the observer executes the communication roles and assists the player in attack mitigation.



High Level Briefings (Workshops And Seminars)

ITU-IMPACT in collaboration with its industry partners regularly conducts high level briefings on current cybersecurity issues, threats and technologies.

Previous sessions have included partners such as Symantec Corporation, Kaspersky Lab, F-Secure, Trend Micro, Microsoft, ABI Research, SANS, Cyber Defense League, and Guardtime and have touched on issues of critical infrastructure protection, phishing, botnets, the Estonian cyber attacks, and offensive cyber counter measures.

International Telecommunication Union (ITU)
Place des Nations, 1211 Geneva 20
Switzerland

Phone	+41 22 730 5111
Fax	+41 22 733 7256
Email	cybersecurity@itu.int
Web	www.itu.int

www.facebook.com/pages/ITU/103018419782973

IMPACT
Jalan IMPACT,
63000 Cyberjaya, Malaysia

Phone	+60 (3) 8313 2020
Fax	+60 (3) 8319 2020
Email	internationalcooperation@impactalliance.org
Web	www.impactalliance.org

www.facebook.com/impactalliance

For more information on our services, please email us at internationalcooperation@impactalliance.org

INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER THREATS
IMPACT