“The Cyber Security Challenge: What Can be Done?”

Lions Club Zürich Metropole

7 June 2016

Presentation by Daniel Stauffacher
President, ICT4Peace Foundation
www.ict4peace.org

ICT for peace foundation

ICT for peace foundation

ICT4Peace is a policy and action-oriented international Foundation. Our purpose is to save lives and protect human dignity through Information and Communication Technology.

We promote cybersecurity and a peaceful cyberspace through international negotiations with governments, companies and non-state actors. We also explore and champion the use of ICTs and media for crisis management, humanitarian aid and peace building.

To learn more about our activities and projects: **www.ict4peace.org**

ADVOCACY CAPACITY BUILDING STAKEHOLDER MANAGEMENT TECHNOLOGY DEVELOPMENT

Information and Communication Technology for Peace

The Role of ICT in Preventing, Responding to and Recovering from Conflict

Preface by
Kofi Annan

Foreword by
Micheline Calmy-Rey

By **Daniel Stauffacher, William Drake, Paul Currion and Julia Steinberger**

United Nations

United Nations Information and Communication Technologies Task Force

ICT for peace

The UN World Summit on the Information Society (WSIS) in Geneva 2003 Tunis 2005

•Paragraph 36 of the World Summit on the Information Society (WSIS) Tunis Declaration (2005):

•*"36. We value the potential of ICTs to promote peace and to prevent conflict which, inter alia, negatively affects achieving development goals. ICTs can be used for identifying conflict situations through early-warning systems preventing conflicts, promoting their peaceful resolution, supporting humanitarian action, including protection of civilians in armed conflicts, facilitating peacekeeping missions, and assisting post conflict peace-building and reconstruction* between peoples, communities and stakeholders involved in crisis management, humanitarian aid and peacebuilding."

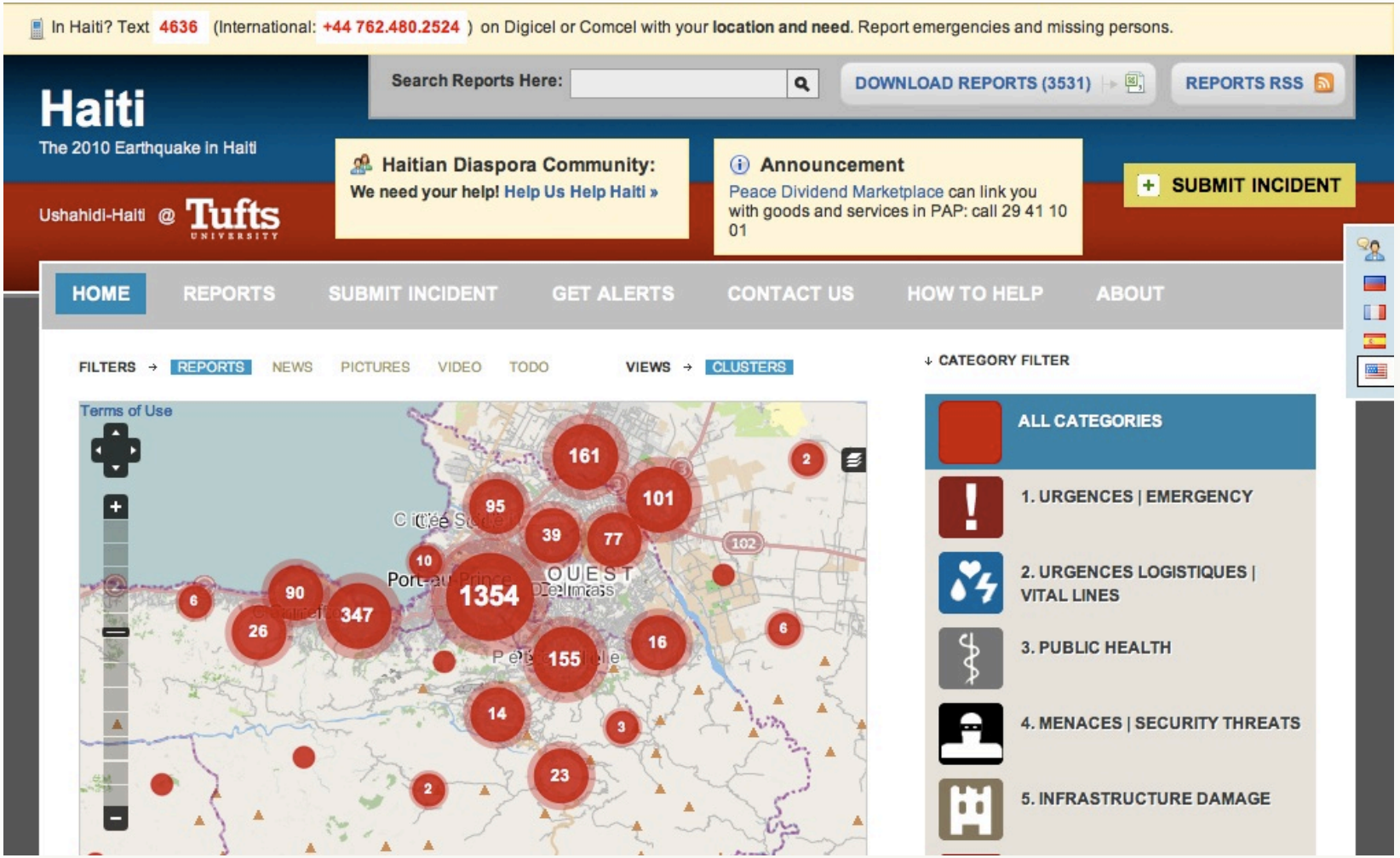
ICT for peace foundation

ICT4Peace interlinked Areas of Work:

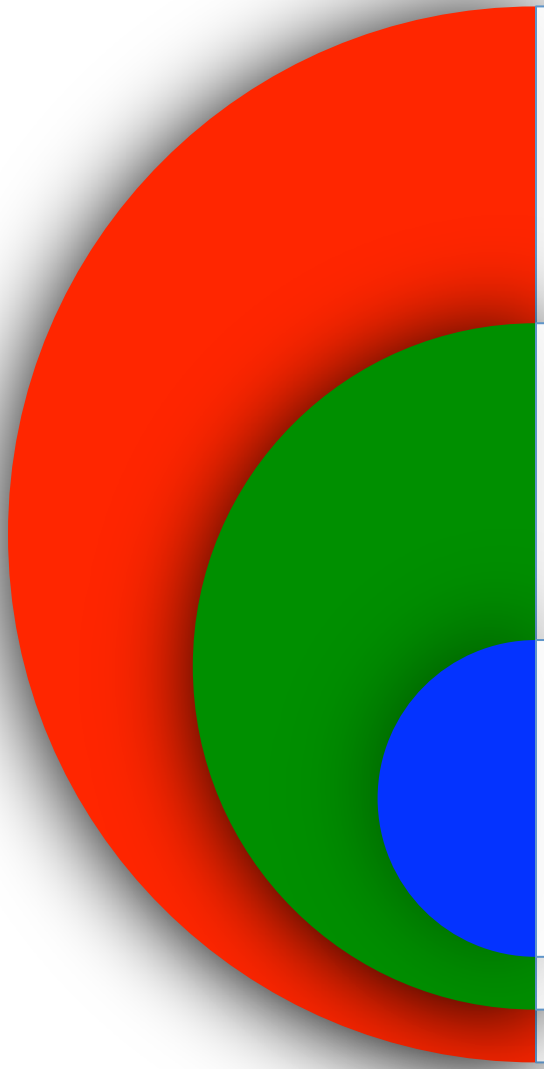
1. CRISIS Information Management including using ICTs, new media etc. at the United Nations

2. Cyber Security

Was ist das ?


In Haiti? Text 4636 (International: +44 762.480.2524) on Digicel or Comcel with your location and need. Report emergencies and missing persons.
Haiti
The 2010 Earthquake in Haiti
Ushahidi-Haiti @ Tufts University
Search Reports Here:
DOWNLOAD REPORTS (3531)
REPORTS RSS
Haitian Diaspora Community:
We need your help! Help Us Help Haiti »
Announcement
Peace Dividend Marketplace can link you with goods and services in PAP: call 29 41 10 01
SUBMIT INCIDENT
HOME
REPORTS
SUBMIT INCIDENT
GET ALERTS
CONTACT US
HOW TO HELP
ABOUT
FILTERS → REPORTS NEWS PICTURES VIDEO TODO
VIEWS → CLUSTERS
Terms of Use
161
101
95
39
77
10
1354
90
347
26
6
155
16
14
3
23
2
102
CATEGORY FILTER
ALL CATEGORIES
1. URGENCES | EMERGENCY
2. URGENCES LOGISTIQUES | VITAL LINES
3. PUBLIC HEALTH
4. MENACES | SECURITY THREATS
5. INFRASTRUCTURE DAMAGE

Information break-down in crisis situation



New media

- Twitter
- Flickr
- Blogs
- SMS / MMS / Mobiles
- **Social networks**
- GIS
- **Crowdsourcing**
- **Drones**

Mainstream media

- CNN / BBC / Al Jazeera
- Local / National TV and radio
- Print media (mainstream / regional)
- Alternative print media

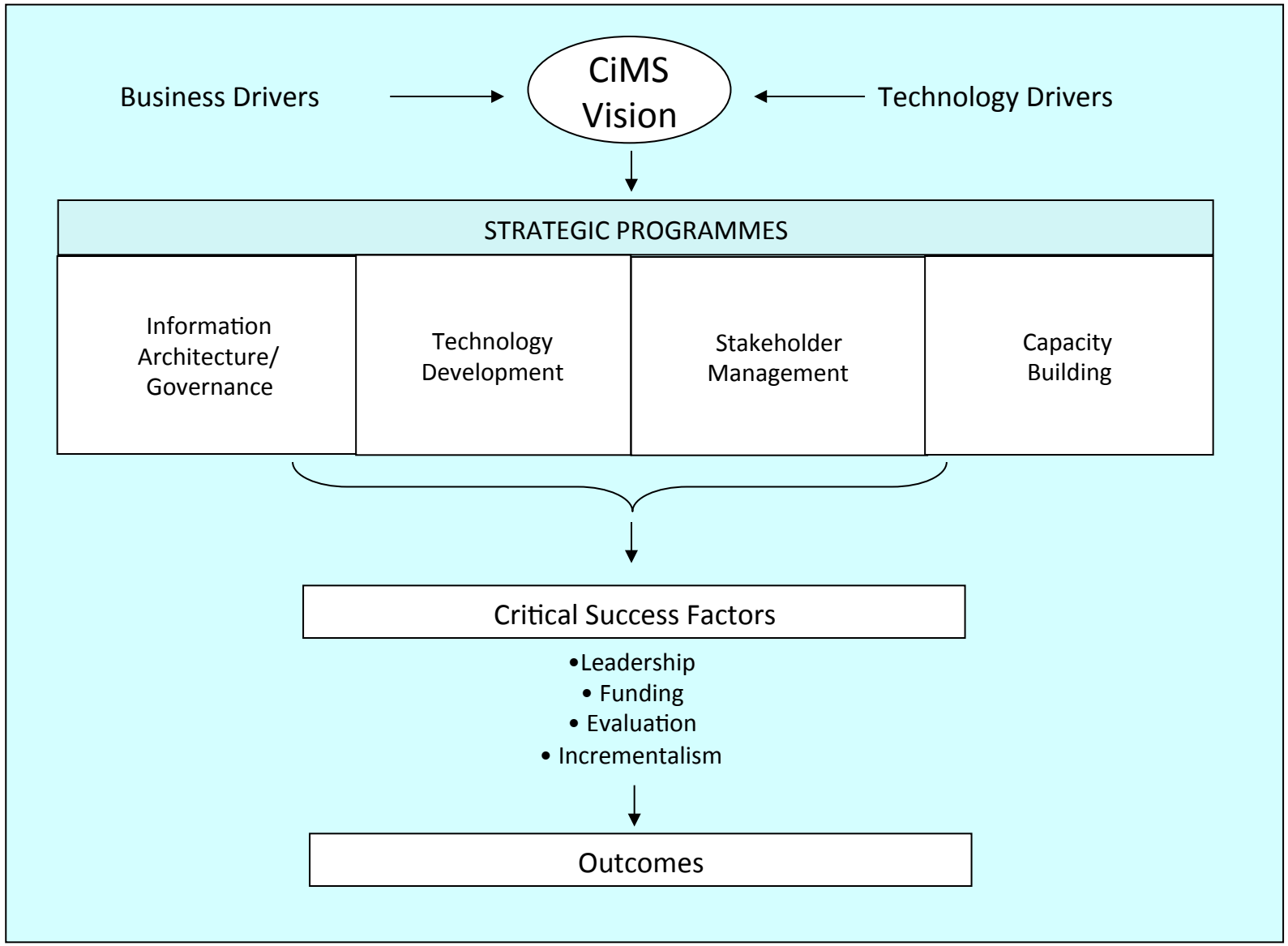
Traditional Sources

- Sit reps
- Open Data Open Gov Data
- Humanitarian Information Centres
- Agency databases / email lists
- Personal contacts / relationships

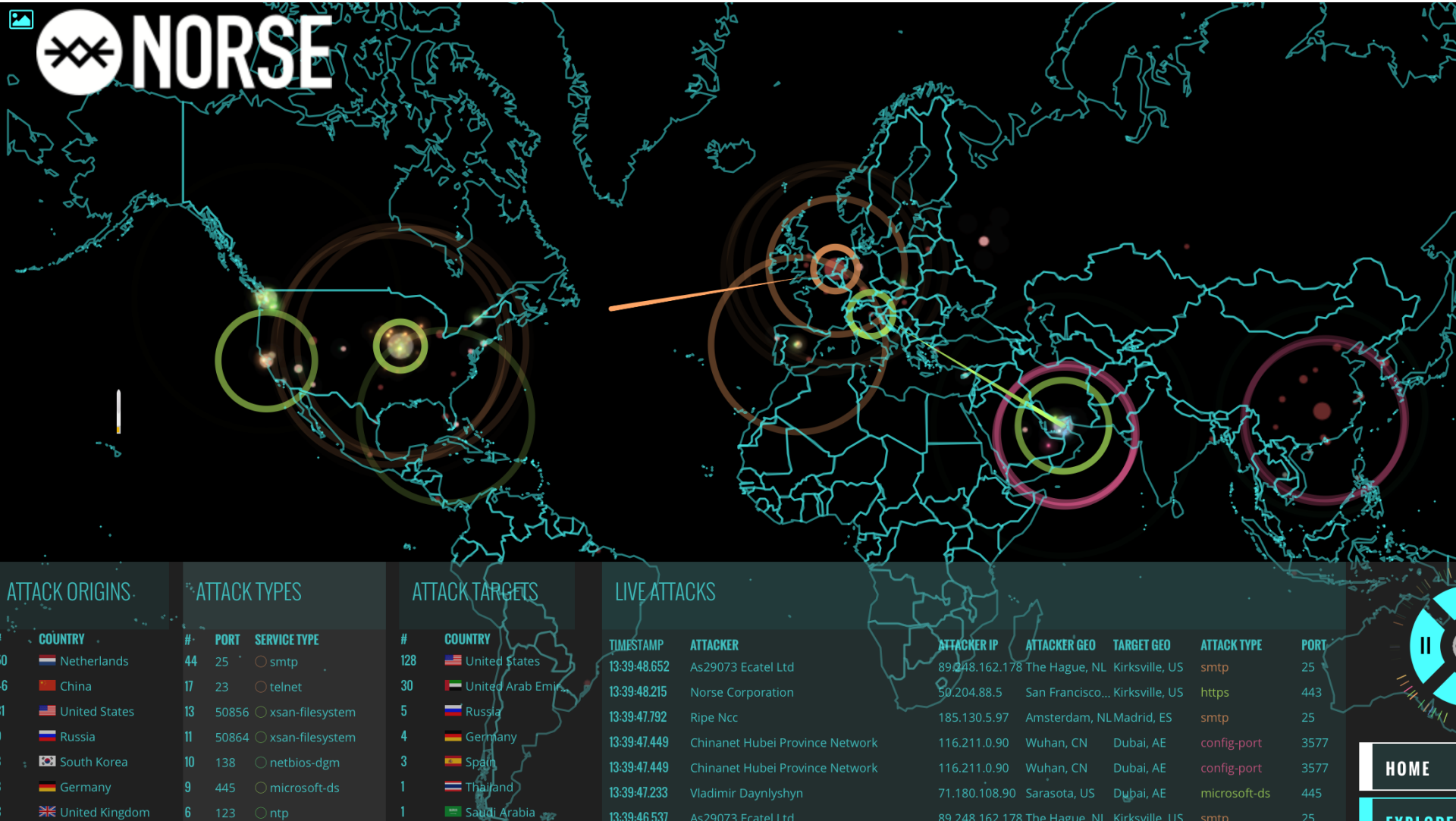
UN Secretary-General 2010 Crisis Information Strategy (A/65/491)

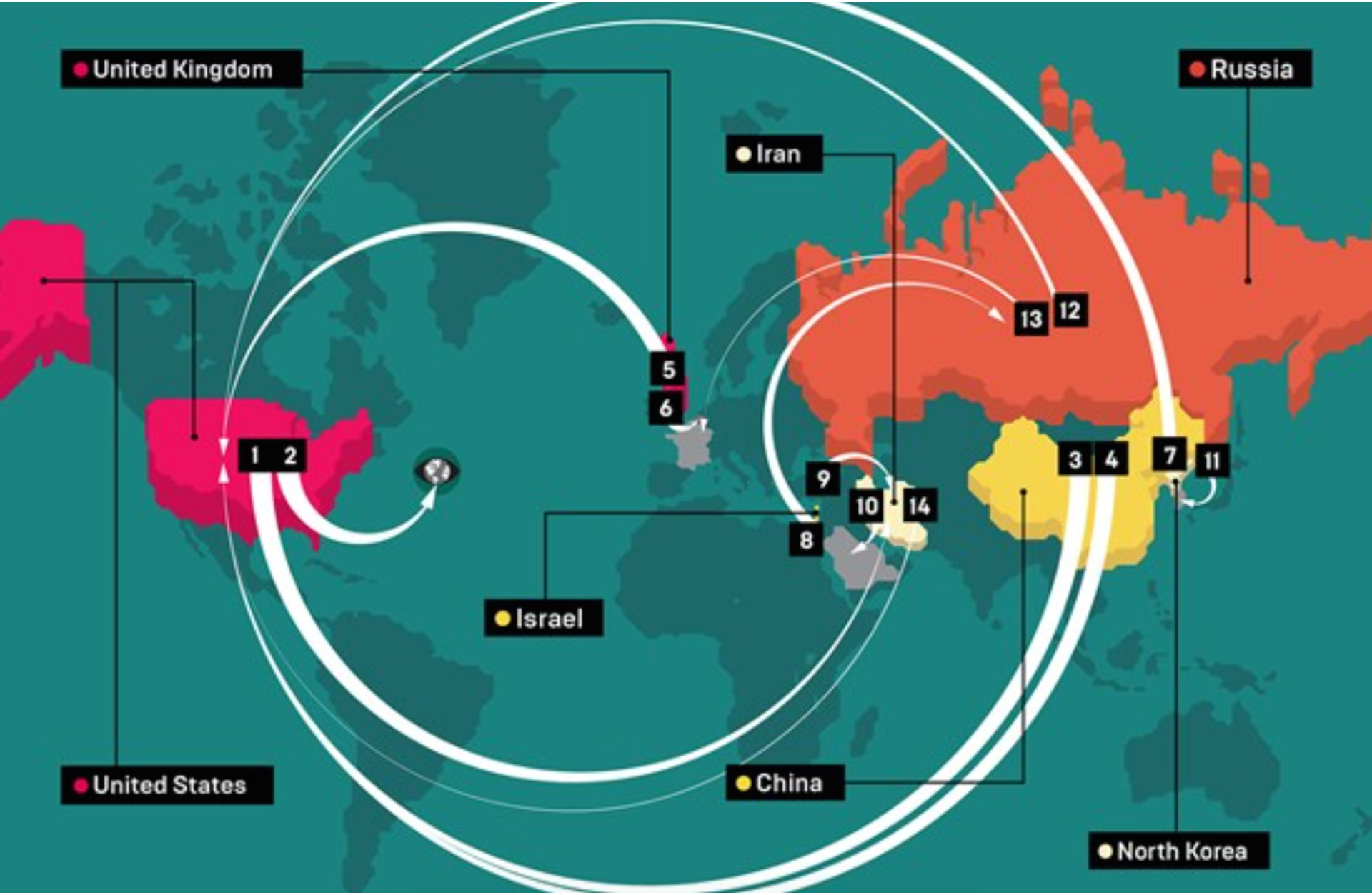
- ***Crisis information management strategy. The Crisis Information Management Strategy is based on the recognition that the United Nations, its Member States, constituent agencies and non-governmental organizations need to improve such information management capacity in the identification, prevention, mitigation, response and recovery of all types of crises, natural as well as man- made.*** *The strategy will leverage and enhance this capacity and provide mechanisms to integrate and share information across the United Nations system.*

- The Office of Information and Communications Technology (CITO), together with the Office for the Coordination of Humanitarian Affairs (OCHA), the Department of Peacekeeping Operations and the Department of Field Suppor (DPKO and DFS), has worked closely with United Nations organizations such as the Office of the United Nations High Commissioner for Refugees (UNHCR), the United Nations Children's Fund (UNICEF), the United Nations Development Programme (UNDP) and WFP and other entities such as **the ICT for Peace Foundation** in developing and implementing this strategy. It is envisaged that membership will be expanded to include other United Nations organizations in the near future.


Business Drivers
CiMS Vision
Technology Drivers
STRATEGIC PROGRAMMES
Information Architecture/ Governance
Technology Development
Stakeholder Management
Capacity Building
Critical Success Factors
•Leadership
• Funding
• Evaluation
• Incrementalism
Outcomes

Was ist das ?


NORSE
ATTACK ORIGINS
COUNTRY
Netherlands
China
United States
Russia
South Korea
Germany
United Kingdom
ATTACK TYPES
PORT SERVICE TYPE
44 25 smtp
17 23 telnet
13 50856 xsan-filesystem
11 50864 xsan-filesystem
10 138 netbios-dgm
9 445 microsoft-ds
6 123 ntp
ATTACK TARGETS
COUNTRY
128 United States
30 United Arab Emi...
5 Russia
4 Germany
3 Spain
1 Thailand
1 Saudi Arabia
LIVE ATTACKS
TIMESTAMP ATTACKER ATTACKER IP ATTACKER GEO TARGET GEO ATTACK TYPE PORT
13:39:48.652 As29073 Ecatel Ltd 89.248.162.178 The Hague, NL Kirksville, US smtp 25
13:39:48.215 Norse Corporation 50.204.88.5 San Francisco... Kirksville, US https 443
13:39:47.792 Ripe Ncc 185.130.5.97 Amsterdam, NL Madrid, ES smtp 25
13:39:47.449 Chinanet Hubei Province Network 116.211.0.90 Wuhan, CN Dubai, AE config-port 3577
13:39:47.449 Chinanet Hubei Province Network 116.211.0.90 Wuhan, CN Dubai, AE config-port 3577
13:39:47.233 Vladimir Daynlyshyn 71.180.108.90 Sarasota, US Dubai, AE microsoft-ds 445
HOME


United Kingdom
Russia
Iran
1
2
5
6
12
13
3
4
7
11
9
10
14
8
Israel
United States
China
North Korea

The Cybersecurity Challenge

- **Many states are pursuing military cyber-capabilities**: **UNIDIR Cyber Index: more than 114** national cyber security programs world-wide, more than **45** have cyber-security programs that give some role to the **armed forces**.

- **A private can obtain, train and use cyber weapons of war.**

- **Damaging of a country's certain critical infrastructure: power, transport, financial sector etc. is possible.**

- **The step from common crime to politically motivated acts, even terrorism, is not far**.

The Cyber Security Challenge: What Can be Done ?

- These scenarios show that we need:
  - to engage in an international discussion on **the norms and principles of responsible state behavior in cyber space**, including on the conduct of cyber warfare, and its possible exclusion or mitigation (UN GGE Tallinn Manual a beginning)
  - **In order to establish a universal understanding of the norms and principles of responsible state behavior in cyber space**, **we need to turn to the United Nations** (such as UN GA, UNGGE, WSIS Geneva Action Line 5)
  - **To prevent an escalation we need to develop Confidence Building Measures** (CBMs) (e.g. Bilateral Agreements, OSCE, ARF, UN GGE)
  - **We need Capacity Building at all levels (policy, diplomatic and technical) to include also developing and emerging countries**

Confidence Building in Cyberspace: Constructive work by UN experts

United Nations A/70/174

General Assembly

Distr.: General
22 July 2015

Original: English

Seventieth session
Item 93 of the provisional agenda*
Developments in the field of information and telecommunications in the context of international security

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

Context of International Security

Note by the Secretary-General

UN Group of Governmental Experts (GGE) on Cybersecurity – 2015: First Set of Peace time norms of responsible behaviour

- GGE report confirmed that 'international law, particularly the UN Charter, is applicable and essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment'.

- A State should not conduct or knowingly support ICT that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public

- States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;

- States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs, and implement other cooperative measures to address such threats.

- At the same time, efforts to address the security of ICTs would need to go 'hand-in-hand with respect for human rights and fundamental freedoms as set forth in the Universal Declaration of Human Rights and other international instruments.

OSCE

Organization for Security and Co-operation in Europe
Permanent Council

PC.DEC/1106
3 December 2013

Original: ENGLISH

975th Plenary Meeting
PC Journal No. 975, Agenda item 1

DECISION No. 1106
INITIAL SET OF OSCE CONFIDENCE-BUILDING MEASURES TO REDUCE THE RISKS OF CONFLICT STEMMING FROM THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES

The OSCE participating States in Permanent Council Decision No. 1039 (26 April 2012) decided to step up individual and collective efforts to address security of and in the use of information and communication technologies (ICTs) in a comprehensive and

Confidence Building Measures: Important Progress at OSCE (CH Presidency)

- Nominating contact points;
- Providing their national views on various aspects of national and transnational threats to and in the use of Information and Communication Technologies;
- Facilitating co-operation among the competent national bodies and exchanging information;
- Holding consultations in order to reduce the risks of misperception, and of possible emergence of political or military tension or conflict that may stem from the use of Information and Communication Technologies;
- Sharing information on measures that they have taken to ensure an open, interoperable, secure, and reliable Internet , and on their national organization; strategies; policies and programs;
- Using the OSCE as a platform for dialogue, exchange of best practices, awareness-raising and information on capacity-building;

BILATERAL EFFORTS IN THE FIELD OF INTERNATIONAL AND REGIONAL SECURITY
Track 1, 1.5 and 2 Dialogues

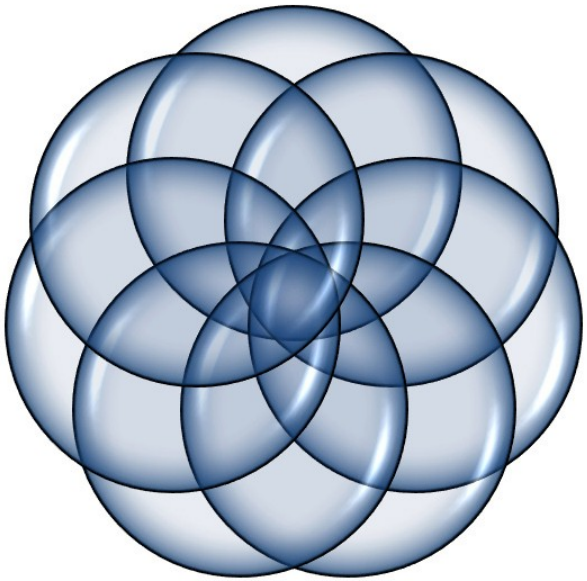
UNITED STATES
- Brazil
- China
- India
- Japan
- Russia
- Sth. Korea

UNITED KINGDOM
- China
- India

SOUTH KOREA
- US
- India

RUSSIA
- US
- India
- Brazil

BRAZIL
- Russia
- US

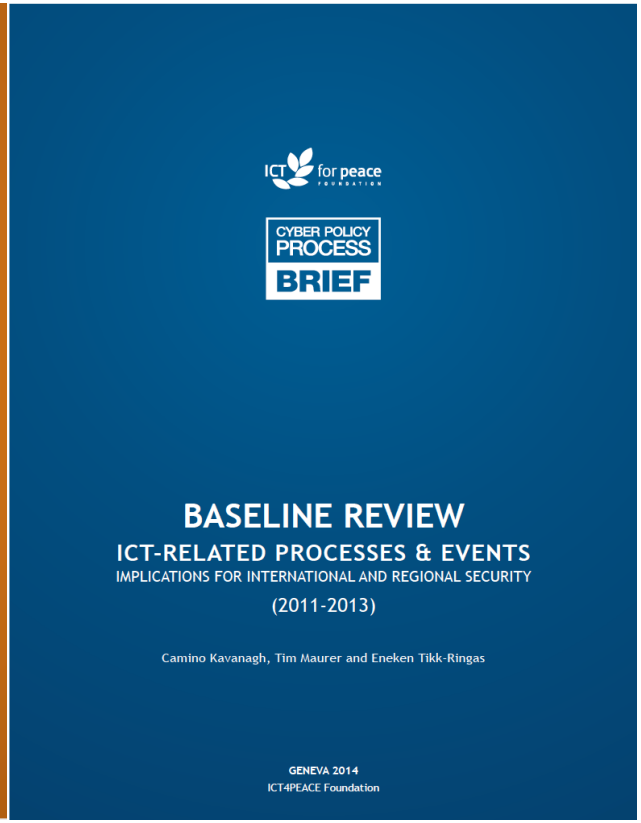


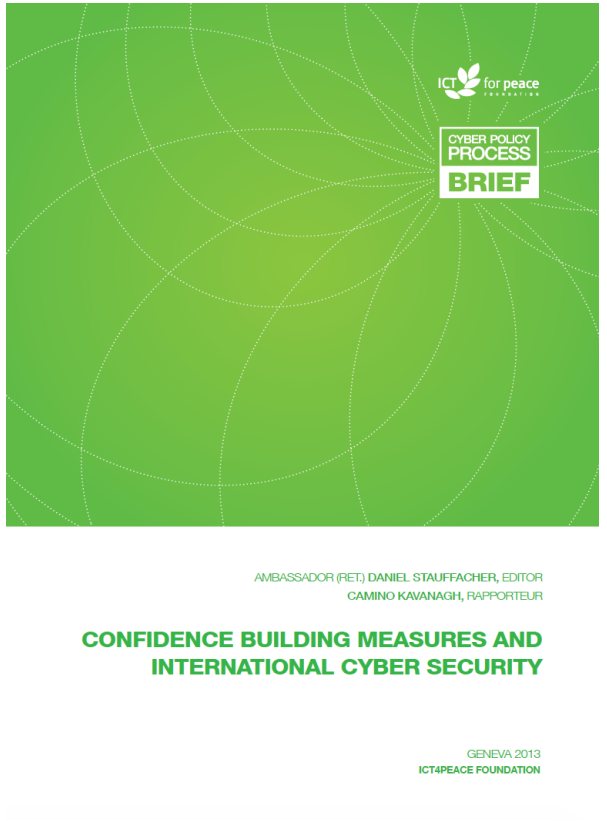
CHINA
- UK
- US
- EU
- Germany

GERMANY
- US
- India
- China

INDIA
- Germany
- Russia
- US
- UK
- Sth. Korea

ICT4Peace Policy Research on Peace, Trust and Security in Cyberspace





ICT4Peace Cybersecurity policy and diplomacy capacity building program with different regional organisations.

As part of its Capacity Building Program for International Cyber Security Negotiations, ICT4Peace organised in cooperation with the African Union Commission the first cybersecurity policy and diplomacy workshop at The African Union Headquarters in Addis Ababa on 15 and 16 February 2016 (see AU Press release).

43 mid-level and senior diplomats from 28 English and French speaking African Countries and 3 regional organisations participated in the 1 1/2 days workshop. The teaching faculty included high-level diplomats and experts from Kenya, Estonia, Switzerland, Germany, Australia and Finland. The workshop was made possible thanks to the generous financial support from the Government of the UK and the AU Commission. Switzerland, Germany, and Australia made high-level experts available.

The workshop program can be found here. and covered the following areas:

- Current international cyber security policy issues
- National cyber security strategies
- Current cyber security consultations and negotiation efforts at the global, regional and bilateral levels
- Cyber security and international law
- Norms of responsible State behaviour in cyber space
- Confidence Building Measures (CBMs) and the role of international and regional organisations

UN GA THIRD COMMITTEE:

'RIGHT TO PRIVACY IN THE DIGITAL AGE (Snowdon)

- It calls on states to **review procedures, practices and legislation on communications surveillance and "to establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and collection of personal data.**"

- It also asks U.N. human rights chief to present a report to the U.N. Human Rights Council and the U.N. General Assembly on the protection and promotion of the right to privacy in domestic and extraterritorial surveillance and the interception of digital communications and collection of personal data, including on a mass scale.

- At the same time, the challenge of reconciling the occasionally conflicting imperatives of ensuring national security and respecting human rights cannot be ignored by governments or citizens alike. At the multilateral level, the UN will have to begin to address the cyber security issue in a more coherent fashion.

THE ICT4PEACE FOUNDATION TEAM

The Foundation's advisory board consists of a Nobel Peace Laureate, senior diplomats, world-renowned practitioners, industry and domain experts, academics and researchers in the use of ICTs for peacebuilding and humanitarian aid.

Daniel Stauffacher

President

Martti Ahtisaari

Chairman, International Advisory Board

Barbara Weekes

Board Member

Maria Cattaui

Chairperson, ICT4Peace Foundation

Alain Modoux

Vice-Chairperson, ICT4Peace Foundation

Sanjana Hattotuwa

Special Advisor

Nigel Snoad

Board Member

Nitin Desai

Board Member

Shahid Akhtar

Board Member

Dag Nielsen

Board Member

Linton Wells II

Board Member

Michael Møller

Member of the Board, ICT4Peace Foundation

Satish Nambiar

Board Member

Kristiina Rintakoski

Board Member

Juliana Rotich

Board Member

Kamal Sedra

Senior Technical Advisor

ICT4Peace at SDG Summit in New York

ICT4Peace: Smart Use of ICT, the Internet and Universal Access Imperative for Successful Implementation of the SDGs

On 27 September 2015 ICT4Peace participated in the UN Summit on the adoption of Sustainable Development Goals (SDGs) and the 2030 Agenda for Sustainable Development, and contributed to the Interactive Dialogue Session on building effective, accountable and inclusive institutions to achieve sustainable development, co-chaired by H.E. President Michelle Bachelet (Chile) and H.E. President Park Geun-hye (Korea). ICT4Peace's Daniel Stauffacher's full statement can be found here.

The Video recording of his intervention (beginning at 2:03:02) can be found here.

ICT4Peace Capacity Building Program for International Cyber Security Negotiations in Singapore

Participants discussion, *inter alia*, the ways through which technology could help in voter and civic education, the challenges the appropriation of technology in a low bandwidth environment, the challenges around the increasing use of mobile telephon the need to identify stakeholders and key audiences in frameworks of engagement around hate speech monitoring and count

Thank you very much

danielstauffacher@ict4peace.org

Cybersecurity Incidents

(Wired Magazine: http://www.wired.co.uk/magazine/archive/2015/10/start/infoporn-cyberattacks-state-sponsored-hacking)

1. UNITED STATES **2001-2015:** Target: the world. Seriously, the **NSA's reach appears to be limitless, according to documents leaked by Edward Snowden**, which describe a vast hacking operation aimed at subverting the internet's infrastructure.

2. UNITED STATES **2007: The US launched the Stuxnet worm against Iran to sabotage that country's nuclear program**.
Outcome: Stuxnet succeeded in briefly setting back the Iranian nuclear programme. The attack set a precedent for cyberwarfare: countries now launch digital assaults to resolve political disputes.

Cybersecurity Incidents

(according to Wired Magazine)

3. CHINA**2009-2011: China allegedly hacked Google, RSA Security and others to get the source code**. The hackers who breached RSA obtained core data used in the company's two-factor authentication scheme used by governments and corporations.

4. CHINA **2014: China breached several databases belonging to the US Office of Personnel Management**. The hackers stole sensitive data, including Social Security numbers, relating to more than 21 million people who had been interviewed for government background checks.

5. UNITED KINGDOM **2009-2013: The UK hacked Google's and Yahoo's undersea cables to siphon unencrypted traffic**. According to documents leaked by Edward Snowden, the UK accessed data through taps of undersea cables belonging not just to these companies, but to major telecoms too.

Cybersecurity Incidents

(according to Wired Magazine)

6. UNITED KINGDOM **2012:** The **UK's Government Communications Headquarters (GHHQ) hacked Belgacom to monitor all mobile traffic passing through its routers.**

7. NORTH KOREA **2014:** **Sony Pictures Entertainment was attacked.** The US attributed it to North Korea and applied additional sanctions against the country and specific officials.

8. ISRAEL **2014: Israel allegedly hacked Russian security firm Kaspersky Lab to obtain intel on its research about nation-state attacks.** It also struck venues in Europe where the UN Security Council met to negotiate Iran's nuclear programm.

Cybersecurity Incidents

(according to Wired Magazine)

9. ISRAEL **2012: Suspected of launching the Wiper attack against the Iranian oil ministry and the National Iranian Oil Company.**

10. IRAN **2012: Iran allegedly launched a virus called Shamoon against oil conglomerate Saudi Aramco's computers**. US officials blame Iran for the attack but have not produced evidence.

11. NORTH KOREA **2013: Computers in South Korea were struck by a logic bomb that caused data deletion as well as preventing rebooting. South Korea blamed North Korea for the attack but it has never produced solid evidence.**

Cybersecurity Incidents

(according to Wired Magazine)

12 RUSSIA **2014: Russia allegedly hacked the US State Department and the White House. The attackers had access to unclassified emails for President Obama as well as non-public details about his schedule.**

13. RUSSIA **2015: TV5Monde, a French-language broadcaster, is hacked -- reportedly by Russia. A group calling itself the CyberCaliphate took credit, but French officials have pointed the finger at the Kremlin**. The hackers blacked out broadcasting for several hours and posted messages expressing support for ISIS to the TV channel's social-media accounts.

14. IRAN **2011-2012: Iran launched a series of denial--of-service attacks on US banks. Although Izz ad--Din al-Qassam Cyber Fighters took responsibility, US officials claimed Iran was retaliating for Stuxnet and UN sanctions.**