

ICT4Peace: Opportunities and Challenges

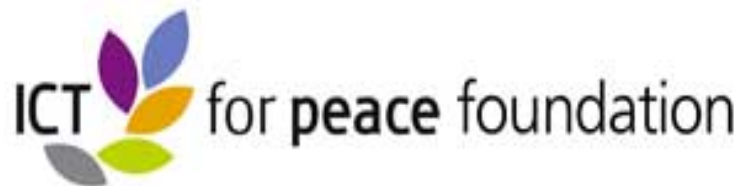
The 12th International Information Security Research Consortium Conference

Seoul, Korea 3 November 2015

Presentation by Dr. Daniel Stauffacher

President, ICT4Peace Foundation

www.ict4peace.org



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

WSIS Tunis 2005
ICT4Peace/UN ICT Task Force
(<http://bit.ly/1bR0yPI>)

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 Currian and Julia Steinberger**



The UN World Summit on the Information Society (WSIS) in 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.



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

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 Cattai

*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 interlinked Areas of Work:

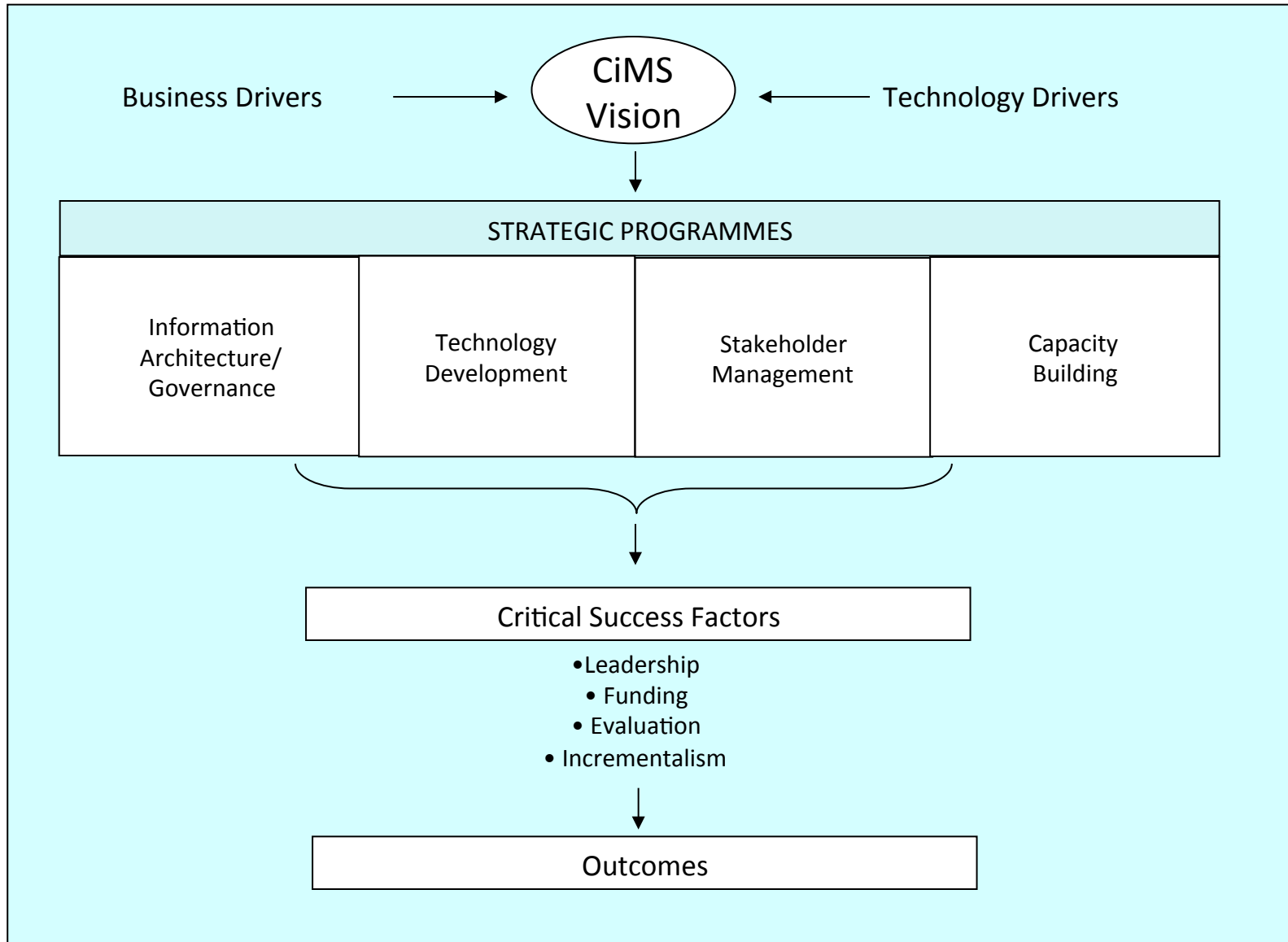
1. CRISIS Information Management including using ICTs, new media etc.

2. Cyber Security Policy and Diplomacy

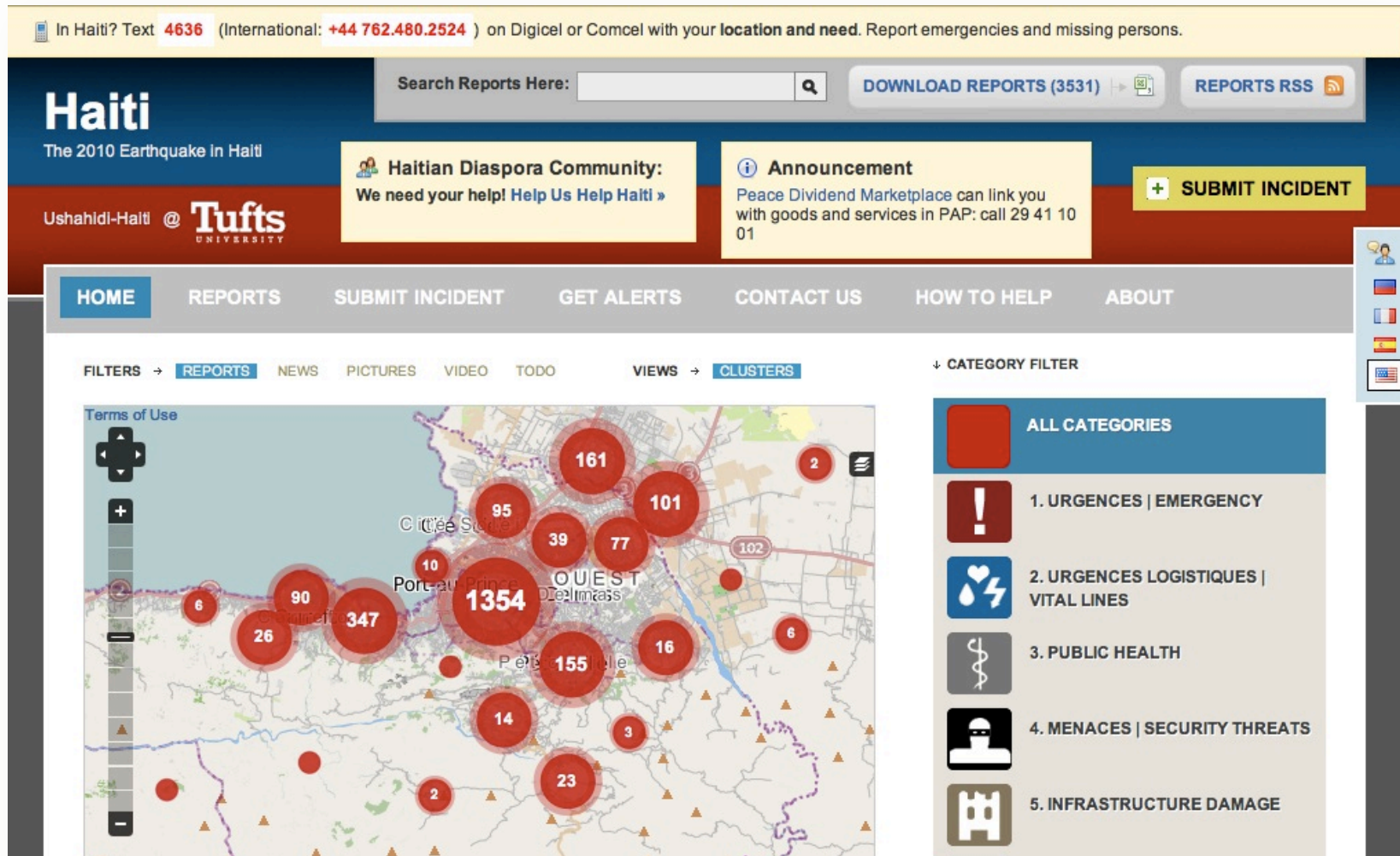


UN Secretary-General 2010 Crisis Information Strategy (A/65/491)

- ***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 Support (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.***



New Tools: Mapping and Crowdsourcing for CiM - Learning from Kenya 2007, Haiti 2010, Libya, Typhoon Yolanda etc. etc.



Improving Crisis Information Management in the Field: MONUSCO



IMPROVING SITUATIONAL AWARENESS Workshop and Training

MONUSCO, Goma, 13 - 15 May 2014

Situational awareness is critical to effective operations and informed decision-making as well as the safety and security of our personnel. Hosted by MONUSCO, in cooperation with the Department of Field Support, and facilitated by the ICT4Peace Foundation, the Improving Situational Awareness Workshop & Training will offer a collaborative forum to discuss information sharing principles, strategies and technologies with MONUSCO practitioners and UN partners.

This three day intensive workshop will introduce participants to new technology tools and platforms used in the collection, verification, and dissemination of information to improve situational awareness. Opportunities for information sharing within the mission and between UN partners will be identified and discussed to develop a practical roadmap for improvement.

CiM Training Course for IM using ICTs and big data, social and new media, ENTRi Course in Cooperation with ZIF and FBA

Navigate a new paradigm: Crisis Information Management Training Course



Folke Bernadotte Academy (FBA), Zentrum für Internationale Friedenseinsätze (ZIF) and ICT4Peace Foundation announce the new Crisis Information Management Training Course at the [International Peace Support Training Center \(IPSTC\)](#), Nairobi from 23 February to 3 March 2013. The Course will teach Information Management practices in Crisis, including Peace and Humanitarian Operations.

A special focus will be given to the use of new Media, including SMS, Twitter, crowd sourcing and crisis mapping to obtain manage and share data. This Course is also linked to the [UN Crisis Information Management Strategy Implementation](#).

For more information, click on the image below.

Course Description

Efficient and timely provision of Shared Situational Awareness (SSA) and Crisis Information Management (CIM) are essential to enable effective decision-making in Multi-



A Breakthrough at UN GA (5th Committee) in December 2014

In December 2014, the UN General Assembly approved the update of the UN Secretary-General's updated Strategy (**A/69/517**), to better exploit the enormous potential of Information and Communications Technologies (ICT) for decision-making and delivery capacity of the United Nations in the areas of peace and security, humanitarian operations and development, human rights and international law.

“Analytics could assist in crisis management efforts and the Office would seek to work with **the Crisis Information Management Advisory Group (CiMAG)** to seek to explore this further.”

Subsequently, the General Assembly in its resolution dated 26 December 2014 (A/C.5/69/L.26*) welcomed the new Information and Communications Technology Strategy in the United Nations, and requested the UN SG to provide, in 2015, detailed information on the implementation.

The General Assembly called on the Secretary-General to continue his efforts to reduce the level of fragmentation of the current information and communications technology environment across the Secretariat and at all duty stations and field missions.

Examples of further ICT4Peace work,
including Using ICTs for election monitoring,
Constitution building etc.



SEARCH



UPDATES



PUBLICATIONS



FEATURED
ARTICLES



KEY REPORTS



ICT4Peace at UN World
Summit on the Information
Society (WSIS) 10 Year
Review Consultations in New
York

2 Nov 2015

ICT4Peace at UN World Summit on the
Information Society (WSIS) 10 Year
...[more](#)

Hate speech, elections and
social media: Presentation for
MIMU in Yangon, Myanmar

30 Oct 2015

At the invitation of the Myanmar
Information Management Unit (MIMU),
...[more](#)

ICT4Peace Capacity Building

Hate speech, elections and social media: Presentation for MIMU in Yangon, Myanmar

Social Media, Hate Speech & Elections

Lessons for Myanmar?

Sanjana Hattotuwa
TED Fellow alumn, ICT4Peace Foundation

At the invitation of the Myanmar Information Management Unit (MIMU), Sanjana Hattotuwa conducted a presentation on the dangers of hate speech and counter-speech as social media and in response. The presentation was based on the strategic deployment of services and counter-speech as well as election monitoring and education.

The discussion lasted a half hour.



ICTs for the prevention of mass atrocity crimes

What is being done to support the prevention of mass atrocity crimes as well as reconciliation, healing and justice with a particular emphasis on the use of Information and Communications Technologies (ICTs)?

ATTACK ORIGINS

#	COUNTRY
354	Saudi Arabia
336	China
168	United States
71	Singapore
44	Russia
43	Brazil
30	Taiwan
17	Netherlands
8	Germany
7	France

ATTACK TYPES

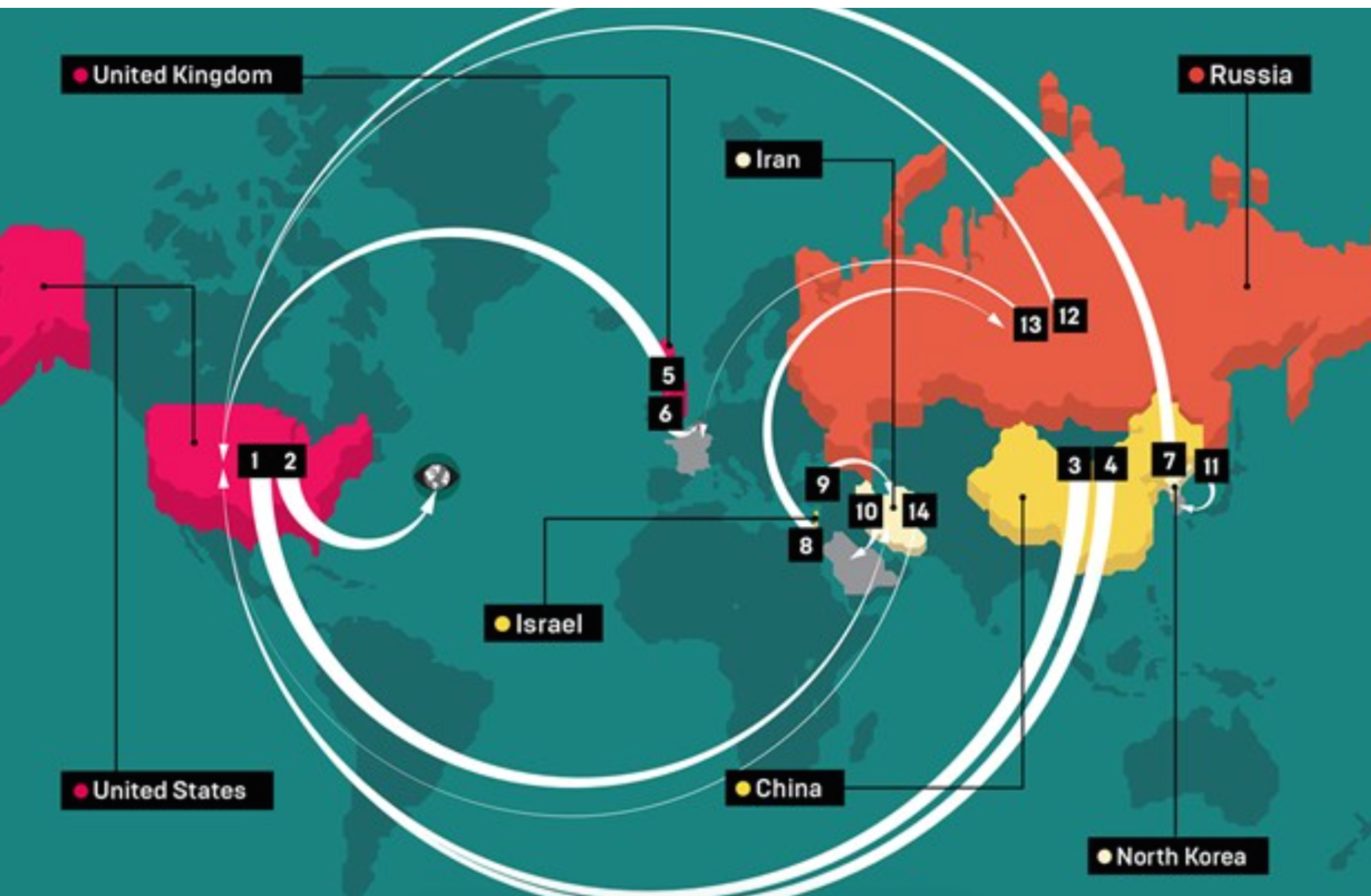
#	PORT	SERVICE TYPE
311	137	unknown
172	23	telnet
88	50864	unknown
69	445	microsoft-ds
55	50856	unknown
38	1500	vlsi-lm
35	33434	unknown
33	27017	unknown
24	443	ssl
21	17	qotd

ATTACK TARGETS

#	COUNTRY
648	United States
354	Saudi Arabia
30	Liechtenstein
30	France
26	United Arab Emirates
20	Russia
15	Taiwan
15	Bulgaria
11	Hong Kong
11	China

LIVE ATTACKS

TIMESTAMP	ATTACKER	ATTACKER IP	ATTACKER GEO	TARGET GEO	ATTACK TYPE	PORT
09:00:24.256	Chinanet Jiangsu Province Network	180.103.193....	Nanjing, CN	Kirksville, US	telnet	23
09:00:24.262	Chinanet Jiangsu Province Network	180.103.193....	Nanjing, CN	Kirksville, US	telnet	23
09:00:24.267	Chinanet Jiangsu Province Network	180.103.193....	Nanjing, CN	Kirksville, US	telnet	23
09:00:24.322	Chinanet Jiangsu Province Network	180.103.193....	Nanjing, CN	Kirksville, US	telnet	23
09:00:24.328	Chinanet Jiangsu Province Network	180.103.193....	Nanjing, CN	Kirksville, US	telnet	23
09:00:24.332	Chinanet Jiangsu Province Network	180.103.193....	Nanjing, CN	Kirksville, US	telnet	23
09:00:24.507	Chinanet Jiangsu Province Network	180.103.193....	Nanjing, CN	Kirksville, US	telnet	23
09:00:24.513	Rn Data Sia	195.3.144.102	Riga, LV	San Francisco, CA	vnc	5900
09:00:24.518	National Computer Systems Co.	46.151.208.26	Riyadh, SA	Riyadh, SA	vlsi-lm	1500
09:00:24.566	National Computer Systems Co.	46.151.208.26	Riyadh, SA	Riyadh, SA	unknown	137



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 Cybersecurity Challenge

- An exclusive, all-out cyber-war **has not happened yet**, but attacks have happened as part of conflicts
- However, Cyber Capabilities **do not fit traditional security strategies** (deterrence, denial), because:
 - Problem of attribution of an attack
 - Rapidly evolving technology produced and in the hands of the private sector
 - Use of Non-State actors, Proxies
- **Arms control agreements (so far) unrealistic** for cyber capabilities
 - Multiple actors, both state and non-state actors
 - No commonly accepted definition of a cyber weapon so 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
 - **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 State 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’.
- The Group noted the proposal of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan for an International Code of Conduct for Information Security, circulated by the Secretary-General as UN document A/69/723.
- 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.

A Comprehensive Normative Approach to Cyber Security

Presented at GCCS 2015



International norms

Legal (binding) norms		Political (non-binding) norms	
Hard law	Soft law		Non-legal norms
Binding norms (treaties, custom, general principles)	Binding norms with a soft dimension*	Non-binding norms of legal relevance*	Non-binding or voluntary norms (e.g. CBMs)

* See Fabien Terpan, *Soft Law in the European Union—The Changing Nature of EU Law*, European Law Journal, Volume 21, Issue 1, pages 68–96, January 2015



**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

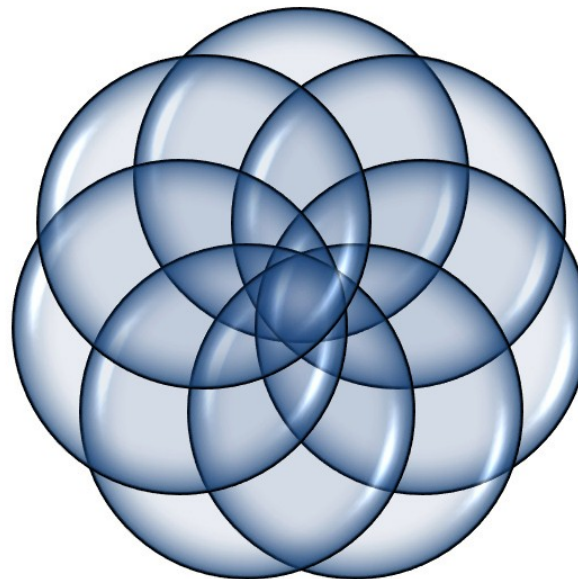
- UK
- US
- EU
- Germany

GERMANY

- US
- India
- China

INDIA

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



ICT4Peace Report on Transparency and Confidence Building Measures (TCBMs)**



** see Report by Camino Kavanagh, Senior Advisor ICT4Peace:

<http://ict4peace.org/what-next-building-confidence-measures-for-the-cyberspace/>

ICT4Peace workshop at ETH Zurich June 2013 with the Support of the Swiss Ministry of Foreign Affairs



BASELINE REVIEW

ICT-RELATED PROCESSES & EVENTS

IMPLICATIONS FOR INTERNATIONAL AND REGIONAL SECURITY
(2011-2013)

Camino Kavanagh, Tim Maurer and Eneken Tikk-Ringas



与信息通信技术相关进程&大事的基本回顾

——对国际和地区安全的影响

(2011-2013)

作者： 卡米诺·卡瓦纳 (Camino Kavanagh)

蒂姆·毛瑞尔 (Tim Maurer)

艾妮肯·提克-瑞格斯 (Eneken Tikk-Ringas)

信息通信技术和平基金会

2014 年·日内瓦



A ROLE FOR CIVIL SOCIETY?

ICTs, NORMS AND CONFIDENCE BUILDING MEASURES
IN THE CONTEXT OF INTERNATIONAL SECURITY

Camino Kavanagh and Daniel Stauffacher



¿UN PAPEL PARA LA SOCIEDAD CIVIL?

TIC, NORMAS Y MEDIDAS DE CONSTRUCCIÓN DE
CONFIANZA EN EL CONTEXTO DE LA SEGURIDAD
INTERNACIONAL

Camino Kavanagh y Daniel Stauffacher

GINEBRA 2014
ICT4Peace Foundation

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

The Government of Kenya and ICT4Peace Foundation co-organize the first Regional Training Workshop in Africa on International Security and Diplomacy in Cyberspace



The ICT4Peace Foundation is honored to have been invited by the Government of Kenya to co-host the first regional training workshop in Africa (2 to 3 March 2015) on International Security and Diplomacy in Cyberspace with over 30 participants (Diplomats, Legal, Security and Technical Staff) from 12 African Countries, the African Union, and Civil Society Representatives. The workshop was co-chaired with Dr. Katherine Getao, Secretary, ICT Authority of Kenya. The Governments of Kenya, the UK, Germany and Switzerland supported the workshop course financially and with lecturers.

This new cyber security capacity building program was developed by the ICT4Peace Foundation as a direct follow-up to some of the recommendations tabled in the 2013 Report of the "UN Group of Governmental Experts on



WSIS+10



**United Nations General Assembly
High-Level Meeting**

[Home](#)

[GA High-Level Meeting](#)

[Preparatory Process](#)

The UN World Summit on the Information Society (WSIS) in 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.

WSIS 2003 Geneva Plan of Action

Follow-up towards WSIS plus 10 in 2015, MDGs and beyond

Action Line C5. Building confidence and security in the use of ICTs

- **12.** Confidence and security are among the main pillars of the Information Society.
- Promote cooperation among the governments at the United Nations and with all stakeholders at other appropriate fora to enhance user confidence, build trust, and protect both data and network integrity; consider existing and potential threats to ICTs; and address other information security and network security issues.
- Governments, in cooperation with the private sector, should prevent, detect and respond to cyber-crime and misuse of ICTs by: developing guidelines that take into account ongoing efforts in these areas; considering legislation that allows for effective investigation and prosecution of misuse; promoting effective mutual assistance efforts; strengthening institutional support at the international level for preventing, detecting and recovering from such incidents; and encouraging education and raising awareness.
- Governments, and other stakeholders, should actively promote user education and awareness about online privacy and the means of protecting privacy.
- Take appropriate action on spam at national and international levels.
- Encourage the domestic assessment of national law with a view to overcoming any obstacles to the effective use of electronic documents and transactions including electronic means of authentication.
- Further strengthen the trust and security framework with complementary and mutually reinforcing initiatives in the fields of security in the use of ICTs, with initiatives or guidelines with respect to rights to privacy, data and consumer protection.
- Share good practices in the field of information security and network security and encourage their use by all parties concerned.

WORLD SUMMIT ON THE INFORMATION SOCIETY
WSIS+10 HIGH-LEVEL EVENT

WSIS+10
OUTCOME
DOCUMENTS

Geneva 2014



JUNE 2014

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT
WORLD SUMMIT ON THE INFORMATION SOCIETY

IMPLEMENTING WSIS OUTCOMES: A TEN-YEAR REVIEW



ICT4Peace Proposal for Zero Draft of WSIS plus 10 Final Document

Under the “Building Confidence and Security in the use of ICTs” section include **a reaffirmation of paragraph 36 of the Tunis Commitment regarding the potential of ICTs to promote peace and to prevent conflict.**

Or a suitable sentence such as: **“Maintaining a peaceful cyberspace and using ICTs as tools for conflict prevention is fundamental to our vision of the information society”.**

Such an affirmation is incumbent on those who wish to prevent conflict from compromising this special environment for humanity and to promote instead the immense contribution ICTs can make in achieving the peacemaking, peacekeeping and peace-building goals of the UN and the international community as a whole

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 (GCHQ) 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.