As cybersecurity becomes a critical issue on the international agenda, there is a growing need for an informed debate on the relationship between governance, security, and fundamental rights and freedoms online, involving all stakeholders. Mapping the main global spaces where cybersecurity is being discussed is an important step towards facilitating greater stakeholder engagement in ongoing cybersecurity debates.

The Freedom Online Coalition (FOC) is a group of governments who have committed to work together to support Internet freedom and protect fundamental human rights – free expression, association, assembly, and privacy online – worldwide. The FOC working group "An Internet Free and Secure" (WG1) seeks to bring a human rights framing to ongoing debates on cybersecurity and aims to develop, through multistakeholder dialogue, meaningful outputs that feed into existing processes.

The mapping was inspired and based upon a visualisation of internet governance processes **"Visualising the playing field"** developed by Deborah Brown, Lea Kaspar and Joana Varon.

The list is not exhaustive, nor do the included processes necessarily work exclusively in the area of cybersecurity. We welcome relevant input related to cybersecurity events, spaces or processes. To propose an addition to the mapping for consideration, please contact:**info@freedomonlinecoalition.com.**

FREEDOM
ONLINE
COALITION

Working Group One

Mapping Cybersecurity

A visual overview of relevant global spaces **in 2015**

May 2015

This mapping of cybersecurity processes and events was developed by members of FOC WG1, and does not reflect the views of the entirety of the FOC membership. It is available online at: **https://www.freedomonlinecoalition.com/**

UN and subsidiary bodies

Within the United Nations General Assembly (**UN**), cyber security-related issues have arisen in the First Committee ("Disarmament and International Security"), the Second Committee ("The Economic and Financial Committee"), and the Third Committee ("Social, Humanitarian & Cultural") of the General Assembly (**UNGA**). Within the First Committee, the Group of Governmental Experts (**GGE**) works on existing and potential cyber threats and possible cooperative measures to address them. The UN World Summit on Information Society (**WSIS**) includes an Action Line on "building confidence and security in the use of ICTs", facilitated by The International Telecommunication Union (**ITU**), a specialized UN agency for information and communica tion technologies. Other UN agencies and subsidiary bodies are also gradually introducing cyber issues into their field of work: the UN Human Rights Council (**HRC**) addresses digital rights, while the Commission on Crime Prevention and Criminal Justice (**CCPCJ**) discusses cybercrime and directs the UN Office on Drugs and Crime (**UNODC**) on the implementation of its work in this area. Most of the UN-related processes are open to delegations of member states or member organisations only, though there is a trend of opening up for participation of other stakeholders.

IGF and related processes

The Internet Governance Forum (**IGF**) is an international multistakeholder forum under the auspices of the UN, established by the Tunis Agenda as one of the outcomes of the 2003/2005 WSIS process. It covers a wide range of Internet public policy issues, cybersecurity being an important one. The agenda of the annual IGF meeting is agreed upon by the Multistakeholder Advisory Group (**MAG**) during the quarterly Open Consultation and MAG meetings, based on the inputs received from the stakeholders; cybersecurity will (again) be one of the main thematic areas of the IGF 2015 meeting in Brazil. Participation is open to everyone and remote or e-participation is strongly encouraged. Regional IGF offspring - the European Dialogue on Internet Governance (**EuroDIG**), the African (**AfIGF**), American, Latin America and the Caribbean (**LACIGF**), Arab (**ArabIGF**) and Asian-Pacific IGF meetings (**APrIGF**) - as well as sub-regional and national, often follow a similar pattern and level of transparency.

Governmental and intergovernmental processes

Governments increasingly view cybersecurity as an important aspect of national security. Besides forming part of bilateral dialogues between states, cybersecurity issues are discussed multilaterally and in inter-governmental organisations including: The Organization for Security and Co-operation in Europe (**OSCE**); the Council of Europe (**CoE**); the African Union; the Organization of American States (**OAS**), the European Union; NATO; the G7; the Shanghai Cooperation Organisation (**SCO**); ASEAN Regional Forum (**ARF**); the BRICS, and the Freedom Online Coalition (**FOC**). Cybersecurity-related discussions have also been part of governmentally-driven processes such as the Wassenaar Arrangement and conferences organised within the framework of the London Process, including the recent Global Conference on Cyberspace (**GCCS**).

Technical and standard-setting bodies

Internet technical and standard-setting organizations such as the Internet Society (**ISOC**), Internet Engineering Task Force (**IETF**), Internet Architecture Board (**IAB**) and World Wide Web Consortium (**W3C**) - are intensifying their work on improving the security standards for Internet infrastructure and protocols, hardware and software. The work of the Internet Corporation for Assigned Names and Numbers (**ICANN**), a non-profit corporation responsible for the global coordination of critical Internet resources (such as the IP numbers and domain names), is of particular interest to the global community. The work of the technical and standard-setting organisations is traditionally open for participation to everyone, including through online tools; the decisions on standards are commonly shaped by "rough consensus" and gradually further refined.

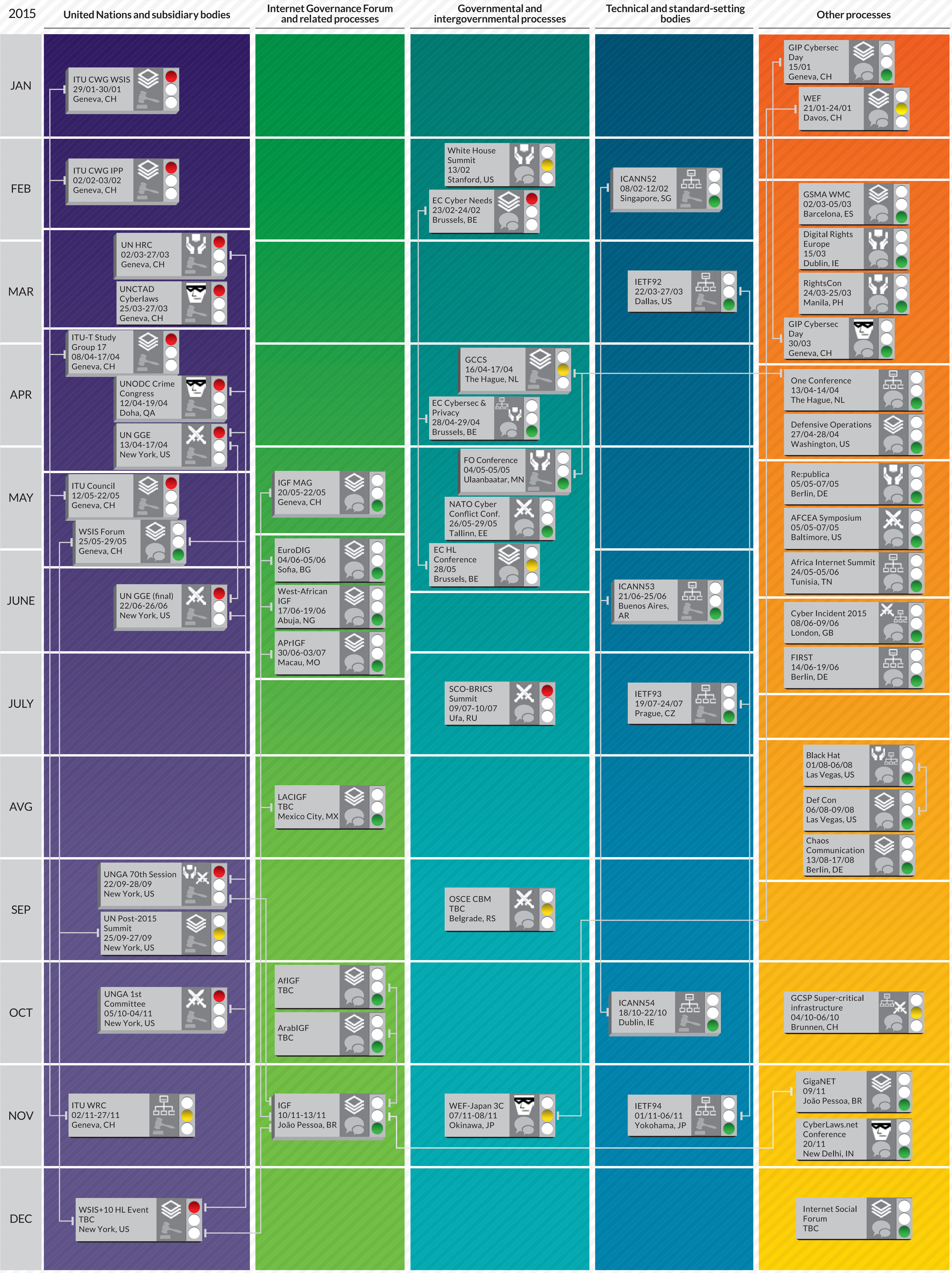
Other processes

Civil society organisations, activists, hacking and technical communities, and academic institutions have long been very active in field of cybersecurity, especially in the discussion of technical gaps, encryption techniques and the protection of digital rights. In addition, they provide invaluable capacity building opportunities and present a source of expertise. The Internet industry and corporations - that is the financial sector and, more recently, the providers of the critical infrastructure (especially the energy sector) - increasingly exchange concerns and experiences both among themselves and with governments and the academic and technical communities. National and corporate incident-response teams (**CERT** or **CSIRT**), which are assembled in associations such as the global Forum for Incident Response and Security Teams (**FIRST**) or the European Union Agency for Network and Information Security (**ENISA**), provide awareness-raising of the risks, offer best practices and assist countries and institutions to build and skill their own teams. Furthermore, law enforcement authorities gathered within Interpol and similar regional forums meet regularly to exchange experiences and improve cooperation and capacities.

List of abbreviations
(if not mentioned above)

EC - European Commission
GCSP - Geneva Centre for Security Policy
GIP - Geneva Internet Platform
GSMA WMC - GSM Association World Mobile Congress
ITU CWG IPP- ITU Council Working Group on International Internet-related Public Policy Issues
ITU CWG WSIS - ITU Council Working Group on WSIS
ITU WRC - ITU World Radiocommunication Conference
OSCE CBM - OSCE Confidence Building Measures
UNCTAD - UN Conference on Trade and Development
WEF - World Economic Forum

2015 CALENDAR: MAPPING CYBERSECURITY EVENTS AND TRACKS



2015	United Nations and subsidiary bodies	Internet Governance Forum and related processes	Governmental and intergovernmental processes	Technical and standard-setting bodies	Other processes
JAN	ITU CWG WSIS 29/01-30/01 Geneva, CH				GIP Cybersec Day 15/01 Geneva, CH WEF 21/01-24/01 Davos, CH
FEB	ITU CWG IPP 02/02-03/02 Geneva, CH		White House Summit 13/02 Stanford, US EC Cyber Needs 23/02-24/02 Brussels, BE	ICANN52 08/02-12/02 Singapore, SG	GSMA WMC 02/03-05/03 Barcelona, ES
MAR	UN HRC 02/03-27/03 Geneva, CH UNCTAD Cyberlaws 25/03-27/03 Geneva, CH			IETF92 22/03-27/03 Dallas, US	Digital Rights Europe 15/03 Dublin, IE RightsCon 24/03-25/03 Manila, PH GIP Cybersec Day 30/03 Geneva, CH
APR	ITU-T Study Group 17 08/04-17/04 Geneva, CH UNODC Crime Congress 12/04-19/04 Doha, QA UN GGE 13/04-17/04 New York, US		GCCS 16/04-17/04 The Hague, NL EC Cybersec & Privacy 28/04-29/04 Brussels, BE		One Conference 13/04-14/04 The Hague, NL Defensive Operations 27/04-28/04 Washington, US
MAY	ITU Council 12/05-22/05 Geneva, CH WSIS Forum 25/05-29/05 Geneva, CH	IGF MAG 20/05-22/05 Geneva, CH	FO Conference 04/05-05/05 Ulaanbaatar, MN NATO Cyber Conflict Conf. 26/05-29/05 Tallinn, EE EC HL Conference 28/05 Brussels, BE		Re:publica 05/05-07/05 Berlin, DE AFCEA Symposium 05/05-07/05 Baltimore, US Africa Internet Summit 24/05-05/06 Tunisia, TN
JUNE	UN GGE (final) 22/06-26/06 New York, US	EuroDIG 04/06-05/06 Sofia, BG West-African IGF 17/06-19/06 Abuja, NG APrIGF 30/06-03/07 Macau, MO		ICANN53 21/06-25/06 Buenos Aires, AR	Cyber Incident 2015 08/06-09/06 London, GB FIRST 14/06-19/06 Berlin, DE
JULY			SCO-BRICS Summit 09/07-10/07 Ufa, RU	IETF93 19/07-24/07 Prague, CZ	
AVG		LACIGF TBC Mexico City, MX			Black Hat 01/08-06/08 Las Vegas, US Def Con 06/08-09/08 Las Vegas, US Chaos Communication 13/08-17/08 Berlin, DE
SEP	UNGA 70th Session 22/09-28/09 New York, US UN Post-2015 Summit 25/09-27/09 New York, US		OSCE CBM TBC Belgrade, RS		
OCT	UNGA 1st Committee 05/10-04/11 New York, US	AfIGF TBC ArabIGF TBC		ICANN54 18/10-22/10 Dublin, IE	GCSP Super-critical infrastructure 04/10-06/10 Brunnen, CH
NOV	ITU WRC 02/11-27/11 Geneva, CH	IGF 10/11-13/11 João Pessoa, BR	WEF-Japan 3C 07/11-08/11 Okinawa, JP	IETF94 01/11-06/11 Yokohama, JP	GigaNET 09/11 João Pessoa, BR CyberLaws.net Conference 20/11 New Delhi, IN
DEC	WSIS+10 HL Event TBC New York, US				Internet Social Forum TBC

1. RELATED THEMATIC AREA

- Cybercrime (crime, safety, child protection)
- International peace and security (arms control, warfare and defence, CBM)
- Multiple (broad cybersecurity, Internet governance, other)
- Network and information security (technology, incident -handling, critical resources)
- Digital rights (privacy and freedoms)

2. LEVEL OF INCLUSIVENESS

- 🔴 Closed (members/invitees only)
- 🟡 Limited (specific conditions)
- 🟢 Open (everyone)

3. FUNCTIONAL MECHANISM

- Decide (directly or within the process)
- Discuss

CONTENT OF EVENT BOX

Title, Date, Place | 1. | 2. | 3.