Group of Seven (G7)

Last Updated: May 2021

Member States

POLICY

Strategy Documents

G7 Principles and Actions on Cyber

- Endorsed by the G7 Leaders at the G7 Ise-Shima Summit
- Key sections and provisions include:
  - **Cyberspace we seek**: reaffirm fundamental role of the free flow of information for promoting the global economy and development; reaffirm the importance of respecting and promoting privacy, data protection and cyber security; emnpasize the G7's commitment to a multi-stakeholder approach to Internet governance
  - **Promoting security and stability in cyberspace:** pledge to take decisive and robust measures against malivious use of cyberspace both by states and non-state actors; stress the importance of close cooperation and collaboration, both nationally and internationally, of the various actors responsible for cyber security, cyber defense and fighting cybercrime; affirm applicability of international law, including the UN Charter, in cyberspace; support the continued development and implementation of cyber CBMs between states; recognize the states' inherent right to self-defense in response to an armed attack through cyberspace
  - **Promoting Digital Economy:** continue to support ICT policies that preserve the global nature of the Internet, and oppose data localization requirements that are unjustifiable taking into account legitimate public policy objectives; endeavor to develop policy frameworks that further promote effective privacy and data protection across jurisdictions, and welcome proactive approaches such as “Privacy by Design”
  - **G7’s concerted Actions:** endeavor to strengthen cooperation to promote security and stability in cyberspace, including through the promotion of cooperation among national CIRTs, capacity building, and awareness raising; commit to enhance cybersecurity threat information sharing and to cooperate for improvement of cybersecurity of critical infrastructure such as finance, energy, transportation, and telecommunication

Source Source 2

27 May 2016

G7 Charter for the Digitally Connected World

G7 ICT Ministers

- Adopted at the G7 ICT Ministers' Meeting in Takamatsu, Kagawa, Japan on 30 April 2016
- Scope and structure:
  1. Provides the set of the G7 countries' Common Goals for realizing sustainable and inclusive development in the digitally connected world, and reaffirms their intention to cooperate on addressing the global challenges that we now face
  2. Provides the set of reaffirmed and shared Fundamental Principles underpinning the digitally connected world
  3. Provides the set of Strategies to realize the potential of the digitally connected world
- Fundamental Principle ii. "Promoting and protecting the free flow of information" *inter alia* aims at respecting applicable frameworks for privacy and data protection, and strengthening digital security
- Strategy II "Strengthening international collaboration for promoting the free flow of information, privacy protection and cybersecurity" aims at fostering efforts to:
  a. Promote cross-border information flows
  b. Promote privacy and data protection; and
  c. Promote cybersecurity

Source Source 2

30 April 2016

Other Documents

Chair's Report of the Meeting of the G7 Ise-Shima Cyber Group

Ise-Shima Cyber Group

- Summarizes the work of the G7 Ise-Shima Cyber Group established following the decision of the G7 Leaders at the G7 Ise-Shima Summit on 26 May, 2016
- Published at the G7 Foreign Ministers meeeting in Toronto, Canada, on 23 April, 2018
- In the Chair's Report, the Group:

Group of Seven (G7)

Last Updated: May 2021

- Noted that threats to the accessible, open, interoperable, reliable and secure cyberspace are on the rise; and that States, their proxies and non-state actors are undertaking malicious cyber activity intended to undermine democratic process and institutions, as well to threaten critical infrastructure and the economic well-being of liberal democracies around the world
- Noted with concern the decline of Internet freedom, including the growing use of Internet shutdowns, restrictions on the use of virtual private networks, restrictions on access to information and freedom of expression, violation of the right to privacy and cyber attacks on journalists, human rights workers, democracy activists and civil society groups
- Recalled the statements and commitments made in the G7 Lucca Declaration on Responsible State Behavior in Cyberspace, including in particular:
  - the call for increased international cooperation on cyber security
  - the commitment to conflict prevention and the peaceful settlement of disputes
  - the applicability of existing international law and the promotion of voluntary, non-binding norms of responsible state behavior in cyberspace during peacetime
  - and the call upon all States to be guided in their use of ICTs by the cumulative reports of the UN GGEs

Source

Undated, published on April 23, 2018

G7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector (G7FE-Assessment)

G7 Cyber Expert Group

- Follow-up on the 2016 G7 Fundamental Elements of Cybersecurity for the Financial Sector
- Promotes the effective practices outlined in the 2016 G7 Document by focusing on how well these practices are performed and assessed
- Includes:
  - Part A: a set of desirable outcomes that a mature entity would likely exhibit and that less mature entities can aim for
  - Part B: a process for their assessment and review
- Desirable outcomes:
  1. The Fundamental Elements (G7FE) are in place
  2. Cybersecurity influences organizational decision-making
  3. There is an understanding that disruption will occur
  4. An adaptive cybersecurity approach is adopted
  5. There is a culture that drives secure behaviors
- Asessment Components:
  1. Establish clear assessment objectives
  2. Set and communicate methodology and expectations
  3. Maintain a diverse toolkit and process for tool selection
  4. Report clear findings and concrete remedial actions
  5. Ensure assessments are reliable and fair

Source Source 2

20 October 2017

G7 Fundamental Elements of Cybersecurity for the Financial Sector (G7FE)

G7 Cyber Expert Group (CEG); G-7 Finance Ministers and Central Bank Governors

- Designed for financial sector private and public entities to tailor to their specific operational and threat landscape, role in the sector, and legal and regulatory requirements
- Serve as the building blocks upon which an entity can design and implement its cybersecurity strategy and operating framework, informed by its approach to risk management and culture
- Provide the financial sector entities with a set of non-prescriptive, not legally binding, high-level elements to use when assessing the level of cybersecurity
- Eight elements encompassed:
  1. Element 1: Cybersecurity Strategy and Framework
  2. Element 2: Governance
  3. Element 3: Risk and Control Assessment
  4. Element 4: Monitoring
  5. Element 5: Response
  6. Element 6: Recovery
  7. Element 7: Information Sharing
  8. Element 8: Continuous Learning

Source Source 2

October 2016

Group of Seven (G7)

Last Updated: May 2021

G7 Fundamental Elements for Threat-Led Penetration Testing (G7FE-TLPT)

G7 Finance Ministers and Central Bank Governors

- Adopted at the G7 Finance Ministers and Central Bank Governors' Meeting in Bali, Indonesia, on 11 October 2018
- Developed as a part of the G7 effort to continue promoting the development of frameworks to enhance public and private sector approaches to strengthening cyber resilience of critical entities in the financial system after publishing G7FE in 2016 and G7FE-Assessment in 2017
- Designed to provide a guide to:
    - (i) authorities considering the use of Threat-Led Penetration Testing (TLPT) for the design, implementation and management of TLPT in their respective jurisdictions
    - (ii) entities undertaking TLPT
    - (iii) organizations providing cyber threat intelligence services ('threat intelligence providers')
    - (iv) organizations providing penetration testing services ('penetration testing providers'); and
    - (v) accreditation and certification providers
- Core objectives are to enhance and assess the cyber resilience of entities and the financial sector more generally, by:
    1. Providing core elements of and approaches for the conduct of TLPT across G-7 jurisdictions
    2. Providing a guide to authorities considering the use of TLPT within their jurisdiction
    3. Providing a guide to entities with respect to conducting their own TLPT assessments; and
    4. Supporting cross-authority interaction and cross-jurisdictional TLPT for multinational entities, facilitating mutual acceptance of test results

Source Source 2

11 October 2018

G7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector

G7 Finance Ministers and Central Bank Governors

- Adopted at the G7 Finance Ministers and Central Bank Governors' Meeting in Bali, Indonesia, on 11 October 2018
- Developed as a part of the G7 effort to continue promoting the development of frameworks to enhance public and private sector approaches to strengthening cyber resilience of critical entities in the financial system after publishing G7FE in 2016 and G7FE-Assessment in 2017
- A set of non-binding Fundamental Elements for entities to tailor, as appropriate, to their specific risk profiles, operational and threat landscape, role in the sector, and legal and regulatory frameworks
- Consider the Third Party Cyber Risk Management Life Cycle within an individual entity and system-wide monitoring of cyber risk
- Third Party Cyber Risk Management Life Cycle elements and practices:
    1. Element 1: Governance
    2. Element 2: Risk Management Process for Third Party Cyber Risk
    3. Identification of Third Parties and Criticality
    4. Cyber Risk Assessment and Due Diligence
    5. Contract Structuring
    6. Ongoing Monitoring
    7. Element 3: Incident Response
    8. Element 4: Contingency Planning Entities have appropriate contingency plans
    9. Element 5: Monitoring for Potential Systemic Risks
    10. Element 6: Cross-sector coordination

Source Source 2

11 October 2018

G7 Opportunities for Collaboration: Annex to Joint Declaration by G7 ICT Ministers

G7 ICT Ministers

- Developed as Annex to the Joint Declaration by G7 ICT Ministers adopted in Takamatsu, Japan on 30 April 2016
- Aimed at sharing information on opportunities for collaboration where greater international cooperation could be an asset, including:
    1. Promoting access to ICT
    2. Promoting and protecting the free flow of information
    3. Fostering Innovation, and
    4. Using ICT to address global challenges and opportunities
- Cybersecurity related project initiatives welcomed by the G7 members include:
    - Collaboration on the Network Incident Analysis Center for Tactical Emergency Response (NICTER), as a method to observe and analyze threats in the cyberspace to comprehend global trends of malicious activities and to share analysis results in a real-time manner
    - Collaboration on the CyberGreen Project, which is a global collaborative initiative which aims to develop and utilize risk-based common metrics for assessing cyber risks to eliminate bots and vulnerable network servers and make the cyberspace clean and resilient to cyberattack
    - Collaboration among Information Sharing and Analysis Centers (ISACs) and related bodies for the purpose of sharing best practices on

Group of Seven (G7)

Last Updated: May 2021

Critical Information Infrastructure Protection
- Collaboration to support initiatives to enhance open source security, such as the Linux Foundation's Core Infrastructure Initiative (CII)
- International collaboration in the domain of spam and malware intelligence, including greater information sharing between international partners and their respective spam reporting centers

Source Source 2

30 April 2016

Cyber Norm Initiative - Synthesis of Lessons Learned and Best Practices

On 6 April 2019, G7 Foreign Ministers met in Dinard, France, and launched a Cyber Norm Initiative dedicated to sharing best practices and lessons learned on the implementation of previously recognized voluntary, non-binding norms of responsible State behaviour. The norms that are presented in this document have notably emerged during the previous sessions of the United Nations Group of Governmental Experts (GGE) and are a subset of the international cyber stability framework. G7 countries are committed to continuing this work and to sharing views on the full range of important recommendations that have been underlined in GGE reports.

Source

26 August 2019

Communications

G7 Ise-Shima Leaders Declaration

G7 Leaders

- Adopted by the G7 Leaders at the G7 Ise-Shima Summit on 26-27 May 2017
- In the section on Cyber, the G7 Leaders:
  - Support an accessible, open, interoperable, reliable and secure cyberspace as one essential foundation for economic growth and prosperity
  - Pledge to take decisive and robust measures in close cooperation against malicious use of cyberspace, both by states and non-state actors, including terrorists
  - Reaffirm that international law is applicable in cyberspace
  - Commit to promote a strategic framework of international cyber stability consisting of the applicability of existing international law to state behavior in cyberspace, the promotion of voluntary norms of responsible state behavior during peacetime, and the development and the implementation of practical cyber CBMs between states
  - Welcome the report of the UN GGE in 2015 and call upon all states to be guided by the assessments and recommendations of the report
  - Reaffirm that no country should conduct or knowingly support ICT-enabled theft of intellectual property
  - Commit to the protection and promotion of human rights online, and to multistakeholder approach to Internet governance
  - Endorse the G7 Principles and Actions on Cyber, as set out in the Annex to promote and protect an open, interoperable, reliable and secure cyberspace; and decide to establish the Ise-Shima Cyber Group (ISCG)

Source

26-27 May 2017

G7 Declaration on Responsible States Behaviour in Cyberspace (G7 Lucca Declaration)

G7 Foreign Ministers

- Adopted at the G7 Foreign Ministers Meeting in Lucca, Italy on 11 April 2017
- In the Declaration, the G7 Foreign Ministers:
  - Remain committed to promoting a strategic framework for conflict prevention, cooperation and stability in cyberspace, the promotion of voluntary, non-binding norms of responsible State behavior during peacetime, and the development and the implementation of practical cyber CBMs between States
  - Express concern about the risk of escalation and retaliation in cyberspace, stress that the risk of interstate conflict as a result of ICT incidents has emerged as a pressing issue for consideration, and express increasing concern about cyber-enabled interference in democratic political processes
  - Encourage all States to engage in law-abiding, norm-respecting and confidence-building behaviour in their use of ICT, and mention cooperative approaches as contributing to the fight against the use of cyberspace by non-State actors for terrorist and other criminal purposes
  - Continue to call upon all States to be guided in their use of ICTs by the cumulative reports of the UN-GGE
  - Provide the list of 11 voluntary, non-binding norms of State behavior during peacetime articulated in the 2015 GGE report and the 2015 G20 Leaders' Communiqué

Group of Seven (G7)

Last Updated: May 2021

Source Source 2

11 April 2017

Joint Declaration by G7 ICT Ministers (Action Plan on implementing the Charter)

G7 ICT Ministers

- Adopted at the G7 ICT Ministers' Meeting in Takamatsu, Kagawa, Japan on 29-30 April 2016
- Reflects the commitment of the G7 ICT Ministers to take the following actions based on the Charter for the Digitally Connected World to maximize its potential:
  - Promoting access to ICT
  - Promoting and protecting the free flow of information, including:
    - Promoting internet openness and cross-border information flows
    - Promoting privacy and data protection
    - Promoting cybersecurity
  - Fostering innovation
  - Using ICTs to address global challenges and opportunities;
  - Strengthening comprehensive international cooperation and collaboration.

Source Source 2

29-30 April 2016

Joint Communiqué from the G7 Foreign Ministers Meeting 2017

G7 Foreign Ministers

- Adopted at the G7 Foreign Ministers Meeting in Lucca, Italy on 11 April 2017
- In the section on "Cyber" the G7 Foreign Ministers:
  - Recognize the threat of the use of ICTs against critical infrastructure, note increased concern over cyber-enabled interference in democratic processes, and bear in mind the risk of misperceptions and uncontrolled escalation
  - Reaffirm commitment to work within the G7 and other relevant international and multi-stakeholder fora to promote strategic frameworks for conflict prevention, cooperation and stability in cyberspace
  - Reaffirm that the United Nations Charter is applicable to the use of ICTs by States
  - Reiterate support for the UN-GGE process and look forward to a substantial outcome of the 2016-2017 UN-GGE; and also call upon all States to be guided in their use of ICTs by the UN GGE's cumulative reports and take measures to operationalize their recommendations
  - Mention the adoption of the the G7 Declaration on Responsible States Behaviour in Cyberspace, and state that they reinforce their commitment to its strategic framework for conflict prevention, cooperation and stability in cyberspace, as a concrete contribution to peace and security
  - Urge all countries to develop laws, policies and practices that effectively combat cybercrime, including, if possible, to become party to the 2001 Budapest Convention against Cybercrime

Source Source 2

11 April, 2017

G7 Dinard Declaration on the Cyber Norm Initiative

G7 Foreign Ministers

- Adopted at the G7 Foreign Ministers Meeting in Saint Malo, France, on 6 April 2019
- As stated in the Declaration, the G7 States:
  - Remain committed to promoting an open, secure, stable, accessible and peaceful cyberspace for all
  - Recall that the General Assembly has affirmed that international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment
  - Recall the conclusions of the 2010, 2013 and 2015 reports of the UN GGEs on cybersecurity
  - Affirm their willingness to to establish a Cyber Norm Initiative (CNI) dedicated to sharing best practices and lessons learned on the implementation of previously recognized voluntary, non-binding norms of responsible State behavior; and encourage, where possible, other interested partners to join G7 in this endeavor
- As participants of the Cyber Norm Initiative, the G7 States commit to:
  - Encourage better and increased voluntary exchange of information, among ourselves and with others, on the steps taken by our respective states to understand and effectively implement the voluntary, non-binding norms of responsible state behavior in cyberspace and the recommendations contained in the abovementioned reports
  - Share the best practices and lessons learned that will be identified as a result of this process with a wide range of states and other stakeholders
  - Engage with other states to include them in our peer-learning, cooperative, transparency and confidence-building efforts
  - Cooperate to help build the G7 partners' capability to implement the above-mentioned voluntary, non-binding norms and

Group of Seven (G7)

Last Updated: May 2021

recommendations

Source Source 2

6 April 2019

G7 ICT and Industry Ministers' Declaration: Making the Next Production Revolution Inclusive, Open and Secure

G7 ICT and Industry Ministers

- Adopted as an outcome document of the G7 Industry and ICT Ministerial Meeting in Taormina, Italy
- Provides the vision and a set of guiding principles for making the Next Production Revolution inclusive, open and secure, including:
  - The opposition to the generally applicable policies that require access to or transfer of source code of mass market software as a condition of market access while recognising the legitimate interest of Governments in assessing the security of these products
  - The need to improve cybersecurity for the effective protection of citizens and business
- Highlights:
  1. the importance of cyber-security for businesses, in particular for SMEs, based on the promotion of company leadership awareness, an effective risk-based management and security by design approaches as a foundation for trust and confidence in the digital environment
  2. the efficient protection and enforcement of intellectual property rights
- Acknowledges that the cyber risks are concerns shared by the business community, and present an opportunity to adopt robust risk-management practices
- For industry, governments and civil society, stresses the importance of considering a variety of approaches, such as security by design, risk management practices, market-relevant conformity assessments and appropriate security evaluation processes, and enhancing security throughout the value chain, while supporting innovation
- Emphasizes the needs to strengthen the efforts to improve risk management, notably for SMEs, for greater digital security for business
- Underlines the importance of encouraging Governments and industry to work together in order to exchange best practices on tackling cyber threats

Source Source 2

26 September 2017

STRUCTURE

Specialized Agencies

G7 Cyber Expert Group (CEG)

G7 Finance Ministers and Central Bank Governors

- Established in November 2015 as an international coordination platform on cybersecurity to support G-7 Finance Ministers and Central Bank Governors efforts to facilitate coordination across members and develop effective practices for cyber resilience in the finance sector
- Key activities and expected deliverables mandated by the G7 members in 2015-2019 include:
  1. Developing a set of high level and non-binding fundamental elements for effective assessment of cybersecurity (G7FE-Assessment)
  2. Developing a set of non-binding and non-prescriptive fundamental elements for threat-led penetration testing in order to evaluate cyber-security measures adopted in the financial sector (G7FE-TLPT)
  3. Advancing the analysis of the potential vulnerabilities stemming from the interaction with third parties located outside the control perimeter (e.g. service providers) (G7FE - Third Party Cyber Risk Management)
  4. Strengthening the coordination with other critical sectors correlated with the financial system (e.g. energy, TLC)
  5. Elaborating proposals for cross-border cyber-crisis simulation exercises involving G-7 financial authorities (planned for June 2019)

Source Source 2

November 2015 (established)

LEGISLATION

COOPERATION

Meetings

Group of Seven (G7)

Last Updated: May 2021

G7 ICT Ministers' Meeting in Takamatsu, Kagawa

G7 ICT Ministers

- First G7 ICT Ministers´ Meeting in about 20 years
- Discussions held over four sessions:
    1. Innovation and economic growth brought by emerging ICTs
    2. The free flow of information and cybersecurity
    3. Using ICTs to address global challenges and opportunities; and
    4. International cooperation and collaboration
- Three outcome documents successfully adopted:
    - The G7 Charter for the Digitally Connected World
    - Joint Declaration by G7 ICT Ministers (Action Plan on implementing the Charter); and
    - G7 Opportunities for Collaboration (annexed to the Joint Declaration), which summarized the fundamental principles and action plans for achieving the Digitally Connected World
- On the free flow of information and cybersecurity, the G7 ICT Ministers:
    - Agreed to oppose data localization requirements that are likely to hinder the free flow of information (except for cases with legitimate public policy objectives)
    - Agreed that the G7 would strongly oppose any potential use of ICTs for criminal and terrorist purposes
    - To ensure a safe and secure cyberspace, agreed to promote initiatives such as research on methods for analyzing trends of cyber attacks and utilization of common metrics for objectively assessing cyber risks

Source

29-30 April 2016

G7 Industry and ICT Ministerial Meeting in Taormina, Italy

G7 ICT and Industry Ministers

- The agenda included the transformation enabled by digital technologies, advanced robotics and data-driven production processes
- Adopted outcome documents include:
    - G7 ICT and Industry Ministers´Declaration: Making the Next Production Revolution Inclusive, Open and Secure
    - Annex 1 to the Declaration: G7 Common Policy Approaches for SMEs' Competitiveness and Inclusiveness in the NPR
    - Annex 2 to the Declaration: G7 Multistakeholder Exchange on Human Centric AI for Our Societies
    - Annex 3 to the Declaration: G7 Actions for Enhancing Cybersecurity for Businesses
- G7 Actions for Enhancing Cybersecurity for Businesses includes 2 key objectives:
    - Objective 1: Developing and implementing appropriate cyber security risk management practices
    - Objective 2: Enhancing cooperation

Source

25-26 September 2017

Activities

Ise-Shima Cyber Group (ISCG)

G7 Leaders

- Established by the G7 Leaders at the G7 Ise-Shima Summit on 26-27 May, 2016 to enhance the G7 policy coordination and practical cooperation to promote security and stability in cyberspace
- First meeting was held on 14 October, 2016 under the chairmanship of Japan; the discussion was focused on the current cybersecurity environment and on how to promote international law, norms, confidence building measures and capacity building in order to increase stability and security in cyberspace
- The Group's second meeting was scheduled for early 2017
- The Group Chair's report was endorsed and published at the G7 Foreign Ministers meeeting in Toronto, Canada, on 23 April, 2018

Source Source 2

26-27 May 2016 (established); 24 April 2018 (the Group Chair's Report endorsed)

"Cybersecurity: Coordinating efforts to protect the financial sector in the global economy" Conference

Banque de France, French Ministry for the Economy and Finance (hosting parties)

- High-level conference held under the auspices of the French Presidency G7 2019; co-organized by Banque de France and the French Ministry for

Group of Seven (G7)

the Economy and Finance

- Aimed at promoting exchanges of views and experiences, bringing together policymakers, the private sector and regulatory authorities on the issues of developing effective responses to cybersecurity challenges to the G7 coutries' financial sector
- Key discussion topics:
    1. The state of cyber threats weighing on the financial sector today
    2. Challenges for the financial sector in adapting to cyber threats
    3. Improving the resilience of the financial sector through crisis management exercises
    4. How to strengthen international cooperation for cyber security?
- At the conference sessions, participants discussed and promoted the initiative of conducting a G7 joint cross-border cyber crisis management exercise with focus on financial sector in June 2019, coordinated by Banque de France

Source Source 2

10 May 2019