Geneva Internet Platform
DigitalWatch
NEWSLETTER

You receive hundreds of pieces of information on digital policy.
We receive them, too.
We decode, contextualise, and analyse them.
Then we summarise them for you.

EDITORIAL

BREXIT AND THE INTERNET

Brexit challenges a decades-long prevalence of integration as the main economic and social paradigm in Europe. Any setback is likely to affect the Internet as a communication infrastructure of global integration. A concern about fragmentation and disintegration of the Internet is shared by a few recent studies.

More on page 3

OBSERVATORY

DIGITAL POLICY TRENDS THIS MONTH

Security, privacy, and net neutrality were again under focus as several developments continue to have a global impact. Digital economy was discussed by OECD ministers. The IANA stewardship transition process was marked with steady progress.

More on pages 4–5

FREEDOM OF EXPRESSION

ONLINE EXPRESSION ANALYSED BY THE UN SPECIAL RAPPORTEUR

The recent report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression stresses the importance of Internet and technology companies in areas affecting freedom of expression in current global circumstances.

More on page 6

CYBERCRIME

DARK WEB: THE GOOD, THE BAD, AND THE UGLY

A tiny portion of the deep web belongs to the 'dark web' – a space without a centralised structure and with non-indexed and very volatile content that is accessible only with special browsers. What makes this safe haven for criminals particularly resilient?

More on page 7

EURODIG HOLDS 9TH ANNUAL MEETING

The 9th meeting of the European Dialogue on Internet Governance (EuroDIG), held on 9–10 June in Brussels, brought together over 600 participants to discuss a wide range of Internet-related issues identified as being of interest for Internet governance stakeholders in Europe. The presence of many representatives of European governments and EU institutions brought added-value to the discussions on controversial topics such as cybersecurity, surveillance, and human rights.
Read more on page 3.

Credit: EuroDIG | vivianhertz.be

In addition to this newsletter, you can find in-depth coverage on the *GIP Digital Watch* observatory (http://digitalwatch.giplatform.org) and join live discussions on the last Tuesday of every month online, at local hubs, or on the Geneva Internet Platform premises | The *Geneva Digital Watch* newsletter is published by the Geneva Internet Platform and DiploFoundation | Design by Viktor Mijatovic, Diplo's CreativeLab | Contributors to this issue: Stephanie Borg Psaila, Samantha Dickinson, Aye Mya Nyein, Tereza Horejsova, Jovan Kurbalija, Virginia Paque, Roxana Radu, Vladimir Radunovic, Barbara Rosen Jacobson, Emanuele Sacchetto, Sorina Teleanu | Send your comments to digitalwatch@diplomacy.edu. The Brazilian version in Portuguese is available at http://digitalwatch.giplatform.org

ITU Council: 2016 Session

Key digital policy issues were discussed during the 2016 session of the ITU Council which took place from 25 May to 2 June. Among the issues discussed were the sustainable development goals (SDGs) and the possibility of including an 18th goal dedicated to information and communications technologies (ICTs); the setting up of an Expert Group to conduct a review of the 2012 International Telecommunication Regulations (ITRs); and ways of recouping operational costs of the ITU and identifying new sources of revenue. *Read the full report on the GIP Digital Watch observatory.*

11th International Security Forum

The 11th International Security Forum, held on 13–15 June, included a session on Cybersecurity and Governance of the Digital Domain. The 14 June session discussed the misuse of the Internet and threats in cyberspace, the role and responsibility of the private sector, and governmental strategies at national level. It focused on future developments, including infrastructure and services, attacks and threats, cloud computing, encryption, and cables. The panel analysed the current challenges in cyberspace and offered an overview of the current debates. *Read the report on the GIP Digital Watch observatory.*

Human Rights Council – 32nd Session

The 32nd session of the Human Rights Council, which ran from 13 June until 1 July, discussed many issues related to human rights at different levels. The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression presented his report regarding free speech and the digital world during a session on 16 June. He stressed the importance of partnership between governments and the private sector, and underlined that the trend of governments asking private companies to shut down websites because of their content could raise serious concerns about censorship and the limitation of freedom of expression. On 17 June, the Special Rapporteur on the right to education also presented his report on the *Right to Education in the Digital Age*, arguing that 'digital technologies should reduce inequalities in society, not widen them'. *Read more about the report from the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on page 6.*

UNIDIR Cyber Stability Seminar

UNIDIR's Cyber Stability Seminar, held on 17 June, considered how the international community could operationalise and build on previous reports from the United Nations Governmental Groups of Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGEs), and generate momentum for a successful 2016–2017 GGE. The conference brought together diplomats, cybersecurity experts, and academics to discuss and explore how to leverage the GGE process to promote a peaceful, stable, and secure cyber environment. The panellists discussed the development of new cyber norms, the implementation of international law in cyberspace, and potential ways to address malicious cyber tools ahead of the GGE report.

Geneva Internet L@w Research Colloquium

A Research Colloquium was organised on 24 June 2016 by the Faculty of Law of the University of Geneva in the framework of the Internet L@w Summer School (20 June – 1 July). Young academics and researchers presented their research projects on Internet platforms, privacy law, net neutrality, algorithmic accountability, and Internet taxation among others. The projects were commented on by experts from the University of Geneva, Berkman Center for Internet and Society, and the Geneva Internet Platform, among others.

EDITORIAL

CHALLENGES FOR THE INTERNET IN THE POST-BREXIT ERA

Brexit has been viewed by some commentators as a protest vote against the globalisation paradigm. As the Internet is the technological basis for global integration, and the medium through which billions of people experience globalisation, Brexit should make us think more seriously about the future of the Internet. The shifting paradigms of globalisation and integration are likely to directly affect the Internet. Thus, the Internet we have today should not be taken for granted.

This is also an echoing message in recent research and studies dealing with the future of the Internet. The World Bank's report on *Digital Dividends* issued a major warning about clouds in the Internet's blue sky: the gap between the promises of the digital era and its real impact is widening. The World Economic Forum report on *Internet Fragmentation* outlined the risks of technological, governmental, and commercial fragmentation of the Internet, and argued that we may end up with many Internets divided by national, corporate, and other borders. *(Read our analysis of both reports in the January 2016 newsletter.)*

Last week, the Global Commission for Internet Governance joined the chorus of alerts with its *One Internet* report. According to Commission's President Carl Bildt, 'The Internet is at a crossroad. Threats to privacy and other risks that may bring the Internet down are real.' The report argues that a Digital Compact for Digital Society is needed to ensure Internet's future growth and stability.

In the search for new Internet arrangements, the good news is that, while all Internet governance actors may be seen as having legitimate interests, they also have limited power to dominate the policy sphere. A balance of sorts already exists.

Governments have a legitimate interest to protect national security, but their power to control online developments and data flows is limited. For Internet companies, a global Internet is at the core of their business model. In addition, users' trust in online business depends on the protection of data. Companies have the encryption power to protect data, but this power can be reduced if they are legally obliged to provide access to users' data in specific cases. The power of Internet users in the digital realm is largely paradoxical. They can exercise the ultimate power by using or not using specific Internet platforms, but their operational power is limited when compared to that of governments and the business sector, both of which have the means to affect digital policies directly.

This mix of legitimate interests and limited power of the main actors provides some optimism for future Internet developments, even in the context of the post-Brexit pessimism. But compromise does not happen on its own. It requires patient work and awareness that public decisions depend both on logos (rationality) and pathos (emotions).

The above is an adaptation of Dr Jovan Kurbalija's blog post, published on Diplo's website. Read the full version.

EVENT

CYBERSECURITY AND HUMAN RIGHTS DISCUSSED AT THE 9TH EURODIG MEETING

On 9–10 June, the European Internet community gathered in Brussels, for the 9th EuroDIG meeting. EuroDIG is one of the earliest Internet Governance Forum (IGF) initiatives; it functions as a platform for open and inclusive discussions on Internet issues that are of particular concern at European level.

Unlike the global IGF, which needs to observe certain formalities such as high level opening and closing sessions, EuroDIG is freer to experiment with its format. For the opening session, EuroDIG contained short welcoming speeches, followed by 90 minutes of discussion generated by the participants. Participants had been encouraged before the meeting to make a statement about their hopes for the theme of the meeting, 'Embracing the digital (r)evolution'.

The location of this year's EuroDIG, Brussels, ensured that there was a significant number of European government participants. This meant that many of the discussions on privacy and surveillance, which are particularly hot topics in European countries, benefitted from the contribution of regulators, law enforcement agencies (LEAs), and the judiciary in a way that is not often seen in multistakeholder Internet governance discussions.

As noted during some sessions, discussions about cybersecurity and privacy can occur in silos: LEAs, national security experts, and the judiciary tend not to participate in the discussions that non-governmental stakeholders have about the human rights dimensions of security-related activities on the Internet. There was debate about whether or not this was due to reluctance on the side of government or non-governmental participants to invite or participate in discussions initiated by the other side. However, there was agreement that there is a need for more dialogue between those who have legitimate concerns about the need to apply the law to online activities and those who have equally legitimate concerns about the need to protect rights online.

In addition to the sessions on human rights and (cyber)security, this year's EuroDIG also featured discussions on issues related to: access and literacy, innovation and economic development, technical and operational issues, media and content, and development of the Internet governance ecosystem. Workshop and main sessions were summarised in key messages, which will later be presented at the IGF as input from the European community.

DEVELOPMENTS IN JUNE

Global IG Architecture

same relevance

According to the Global Commission on Internet Governance (GCIG), the Internet can evolve in one of three directions: it can become a broken cyberspace, feed unequal gains, or foster unprecedented progress. The GCIG report, presented at the OECD meeting in Cancun in June, claims the Internet's future depends on a 'new social compact'.

Sustainable development

same relevance

The first Multi-stakeholder Forum on Science, Technology and Innovation for the Sustainable Development Goals stressed that enabling environments for science, technology, and innovation are critical to achieve the SDGs.

'ICT will be the difference between attaining the goals and failing to even come close' – the GIP head said in an interview in *The Guardian*.

The Commonwealth's ICT ministers endorsed a strategic plan from the Commonwealth Telecommunications Organisation (CTO) for 2016–2020, underlining the importance of sustainable development through ICTs, and linking the CTO's activities to the SDGs.

Security

increasing relevance

NATO has declared cyberspace its fourth operational domain, in addition to air, land, and sea. The decision will enable NATO to offer protection against cyberattacks, and to develop capabilities to protect countries' cyber networks.

The UK House of Commons has passed a revised version of the Investigatory Powers Bill (Snoopers' Charter), in which companies can be asked to remove encryption that they themselves have put in place, if this is technically feasible and not unduly expensive.

A database of almost 33 million Twitter accounts, and a Windows zero-day flaw, go for sale on the Dark web. *Read more on page 7*

Prime Minister of India Narendra Modi and US President Barack Obama agreed to finalise a Joint Framework for the USA-India Cyber Relationship (focusing on cybersecurity) in the near term.

In a white paper on cybersecurity norms, Microsoft proposes a set of offensive, defensive, and industry norms for both governments and the ICT industry.

Privacy and human rights

increasing relevance

The EU and the USA have agreed on the final changes to the EU-US Privacy Shield. The new framework is expected to be adopted in July.

In Russia, a bill introduced as part of new anti-terrorism laws is proposing mandatory cryptographic backdoors in all messenger applications. Encryption backdoors would enable government authorities to obtain access to all Internet communications within the country.

Online expression is more and more affected by private networks, and by platforms created, maintained, and operated by ICT companies and organisations, as well as governments. The newly released 2016 report from the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression makes seven recommendations, and includes extensive public input.
Read more on page 6

Infrastructure

down relevance

Only 12% of Internet users connect over IPv6, new Google statistics have revealed.

The European Commission plans to modernise the European Standardisation System through a Joint Initiative on Standardisation (a dialogue process to speed up and streamline the standard-setting process), among other initiatives.

As of January 2017, applications in Apple's App Store can only use HTTPS connections. The so-called App Transport Security (ATS) feature will become mandatory for developers.

Net neutrality

increasing relevance

The EU telecom regulators' body BEREC has published draft guidelines on the implementation of new net neutrality rules, aimed at clarifying certain grey areas in the EU net neutrality rules adopted in December 2015. The guidelines suggest that regulators should decide on zero-rating 'depending on the market share of both the operator and the company providing the free content'.

The US appeals court for the District of Columbia Circuit has upheld the net neutrality rules introduced by the Obama administration. The legal battle will continue as telecommunication companies are expected to appeal further.

E-commerce and Internet economy

increasing relevance

During the OECD Cancun meeting, countries agreed on a range of proposals, including using 'multi-disciplinary capabilities [...] to look beyond the ICT sector to look at how to make policies in everything from tax and trade to transport ready for the digital era'.

The European Union has issued non-binding guidelines on the sharing economy, aimed at reaping the benefits of new business models, and addressing concerns over the uncertainty of rights and obligations arising from the sector. Meanwhile, Berlin's administrative court upheld a de facto ban on short-term rentals, affecting Airbnb and other short-term letting agencies.

In India, purchases made online will attract a uniform Goods and Services Tax as of April 2017, according to a newly approved model law; in Russia, a new law is set to impose VAT on foreign Internet companies selling online content.

Jurisdiction and legal issues

same relevance

An Israeli court has approved a $400 million class action against Facebook, and ruled that the California jurisdiction clause in Facebook's terms of use is invalid.

A Paris attack victim's father has accused Google, Facebook, and Twitter of offering 'material support' to terrorists, claiming that they knowingly permitted recruitment of terrorists, fundraising, and the spread of extremist propaganda.

A US appeals court has ruled that video-sharing website Vimeo cannot be held liable for copyright infringement for unknowingly hosting older music uploaded by its users. This represents a win for the online platform, and a blow to record labels.

IANA Transition

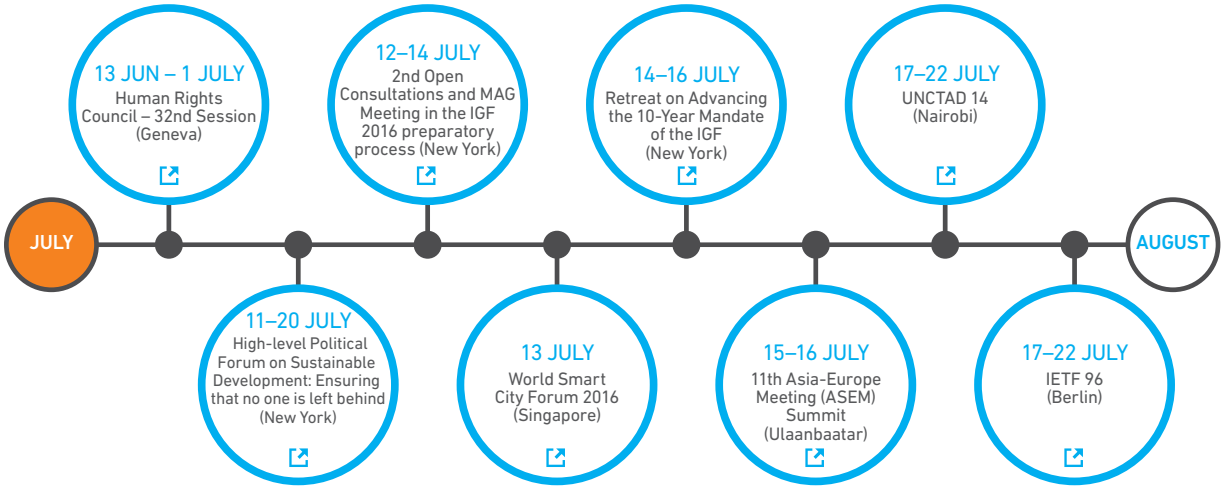
increasing relevance

The NTIA has confirmed that the IANA stewardship transition proposal meets the criteria necessary to complete the privatisation of the IANA functions.

In the USA, Sen. Ted Cruz proposed a bill requiring Congress to approve the IANA stewardship transition to the global multistakeholder community.

The Cross Community Working Group on Enhancing ICANN Accountability (CCWG-Accountability) has started working on additional areas to improve ICANN's accountability (the so-called Work Stream 2).

AHEAD IN JULY



For more information on the IG Barometer, consult www.giplatform.org/barometer

SPECIAL RAPPORTEUR ON FREEDOM OF EXPRESSION: A LOOK AT THE 2016 REPORT

The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression presented his report on the current situation with freedom of expression in the digital era during the 32nd Session of the Human Rights Council in Geneva. Here, we take a look at the main highlights.

Mr David Kaye, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression since August 2014, presented his report on the current situation of freedom of expression in the digital era during the 32nd Session of the Human Rights Council in Geneva from 13 June to 1 July. The report included extensive public input in the form of a review of submissions by 15 countries and 15 civil society organisations, mapping exercises, and expert consultation.

Throughout the report, Kaye stressed the importance of the private sector in areas affecting freedom of expression in current global circumstances, particularly involving online and digital media. This sector, including Internet resources and the ICT applications, has both supported and challenged the right to freedom of opinion and expression, from the business, provider, and user communities, and from state regulations that have the capacity both to protect and to violate these freedoms online and offline. Both the private sector (business) and governments have the means to act as facilitators or gatekeepers of the flow of communication. The report analyses the possible trends, dangers, concerns, and opportunities presented by current technologies, and proposes to map major threats to freedom of expression from the impact of these tendencies. Kaye highlighted the need to support growth of knowledge and information exchange through digital and online technologies.

The main highlights of the report outlined an ongoing review of the current legal and political ecosystem, which is the focus of Kaye's current work. In particular, he outlined the recent cases of Tajikistan and Japan. In the first case, he raised awareness about the numerous threats to and cases of intimidation of journalists in that country, as well as the frequent blocking of information sources on the Internet. In Japan, free press and online freedom of expression are specifically established (art. 21 of the Constitution), but there are still limitations regarding media independence.

David Kaye, UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

Major highlights in the report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression:

• The role and responsibility of the private sector, including the ICT industry, are of vital importance to the protection of the freedom of opinion and expression.

• States must not exercise undue pressure on the private sector to take unnecessary or disproportionate steps to take down digital content or access consumer information; these must be solidly based on due process and valid legal instruments.

• Public access to policies, standards, reports, and other Internet governance information and policies should be proactively facilitated, and transparent procedures implemented, in particular by international organisations.

Kaye particularly underlined the necessity to establish to what extent the private sector and the ICT industry have a responsibility to promote and protect freedom of expression, and identify norms and standards. At the same time, he stressed the problematic trend of governments asking private companies to filter inappropriate content, thus increasing the risk of online censorship. Moreover, this privately exercised process of shutting down is neither clear, nor democratic. He stressed the problem of arbitrariness in the blocking, filtering, and taking down of online content, in the absence of any judicial process, noting the need for a transparent, multistakeholder process to establish clear responsibilities and procedures.

Concluding his report, Kaye defined the steps to work on in the future and the roles of governments and of private companies. In particular, governments must engage in adopting and implementing rules and technical measures to protect freedom of expression and opinion online. They should also refrain from pressuring private companies to take censorship measures, such as taking down websites, without a valid legal basis. He reiterated that the private sector, with multistakeholder support, should develop transparent rules and human rights assessment procedures in order to avoid illegitimate restrictions of freedom of expression.

DARK WEB: THE GOOD, THE BAD, AND THE UGLY

One tiny portion of the deep web belongs to the 'dark web' – a space without a centralised structure and with non-indexed and very volatile content that is accessible only with special browsers. Even though the dark web is often associated with 'the bad', it also contains 'the good' – and 'the ugly'. What makes the dark web particularly resilient?

Each day, over 3.5 billion queries are entered into Google's search engine. Add billions of posts on social media per day, and it becomes clear that the most dominant way we access online content is through search engines and shared links. The 'surface web' that we use every day, however, is estimated to be less than a thousandth of the entire web! The rest is in the 'deep web': invisible content not indexed by search engines. It contains databases, password-protected websites, intranets, academic journals, and archives, some of it being accessible through specific applications or with credentials.

On its good side, the dark web enables the communication of human rights activists and whistleblowers around the world (it has facilitated freedom of expression in Iran and Egypt, and it has been used by Wikileaks and Edward Snowden, as well as by journalists and even officials). But the dark web also hosts markets of illegal goods (such as counterfeit products, drugs, and IDs) and financial crime services (such as money laundering and bank frauds). There is an ugly side to it as well: markets offering paedophilia content, hitman services, weapons purchase, and illegal medical research.

A particularly flourishing offer is of personal information and online credentials (passwords, emails, IDs) and cyber-weapons (exploits, malware kits, and botnets). Each day, the headlines feature such updates, like the recent ones about 32 million Twitter passwords or the new Windows zero-day flaws – all for sale. *Read about the latest updates on page 4.*

The abundance of hacked information and exploits enables the emergence of cheaper and simpler to use, yet more sophisticated malware (such as trojans or ransomware) and social engineering techniques (such as phishing and spear-phishing), and even cyber-attack services (distributed denial-of-service or DDoS attacks, hacking and defacement, spam and malware distribution) – with customer support. For instance, one can rent a smaller botnet for about €100, or a DDoS attack for less than €50 per day; no specific skills are required except for how to find such offers online.

What makes the dark web, including its bad and its ugly parts, particularly resilient is the anonymising dark net tools that allow strong encryption and decentralisation. The most notable are the anonymous peer-to-peer open software networks, Tor (The onion routing) and I2P (Invisible Internet Project), developed to protect personal privacy and freedoms by encrypting and distributing communications, thus preventing traffic analysis and surveillance. While they provide security and even save the lives of activists and journalists working in politically unstable parts of the world, they also provide the ability to hide criminal activities. In addition, crypto-currencies like BitCoin (a decentralised peer-to-peer electronic system of payment), which have great potential for global markets, at the same time enable criminals to transfer money while avoiding the centralised banking system. Each step in a regular crime market between a seller and a buyer (communications and transactions, trust, payment and money flow, and logistics) can be anonymised, which makes it a hard task for law enforcement agencies (LEAs) to combat dark markets.

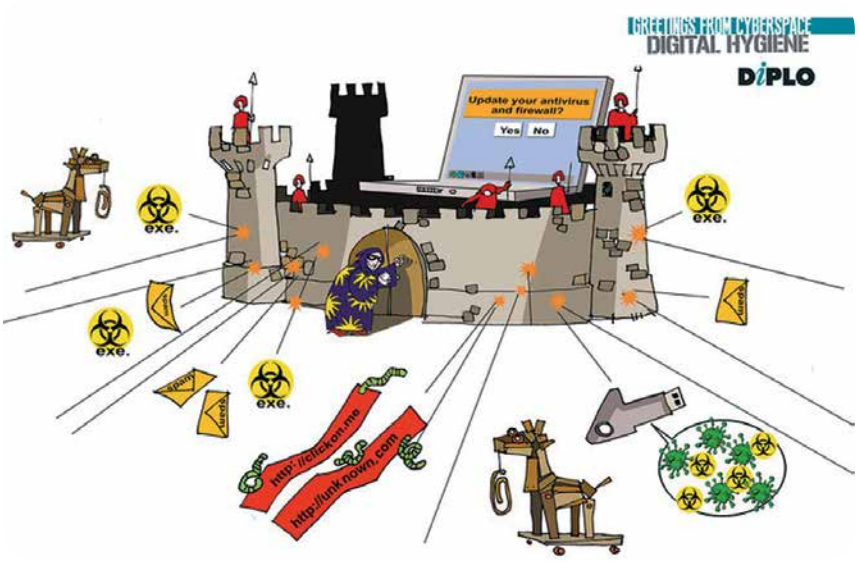
The relatively low risk of conducting criminal operations online encourages the emergence of new dark market platforms. Nevertheless, investigation units, especially the FBI, are building their skills to infiltrate cybercriminal networks, and to make use of the Tor network, in order to mitigate the anonymisation and identify the physical locations of dark market servers and the key individuals operating them. In recent years, the take-down of major illegal drug markets such as Silk Road 1 and Silk Road 2, Evolution, and Agora – and the arrest of some of their key operators – have shown that the operational cooperation of LEAs can bring results, yet it still faces many obstacles across jurisdictions. A harmonisation of national legal environments, such as that based on the Budapest Convention of the Council of Europe, and investment in capacities and human resources of LEAs, can increase the efficiency of taking down the dark markets and help preserve 'the good' of the dark web.

To learn and discuss more about cybersecurity and cybercrime policy, mechanisms, and international cooperation, join Diplo's online course on cybersecurity.

STAYING SECURE IN CYBERSPACE

Criminal techniques have advanced so rapidly that they need only a moment's inattention to get into our computers – by luring us to click on a link to a file or by getting into our device on a public WiFi network – infecting it or accessing and stealing our data. Criminals can use our devices to send virus messages or spam to our contacts, profiling us to access our passwords or security questions, locking all our data and asking for ransom, and much more. To prevent this, we need to perform regular digital hygiene – just like going to a doctor for a check-up, or taking our car in for service. Here are our tips.

Securing your computer is no different to securing your health: along with regular personal hygiene and medical check-ups, perform digital hygiene and check-ups as well.



This illustration is one of a series of cybersecurity-themed postcards designed by Diplo's CreativeLab. The postcards illustrate the main challenges related to cybersecurity, and are aimed at raising awareness about related issues. View the gallery.

Stay secure with one-off precautions:

- Set your Firewall and system (Windows) update.
- Install an antivirus (free versions include Avast! and AVG).
- Disable Macros when using MS Office.
- Verify your Google, social media, and other accounts through SMS, and set security questions.
- Use complex passwords; if you use a password manager, make sure your master password is very strong and change it often.
- Where possible and convenient, use two-factor-authentication (a combination of username/password and a one-time code received by SMS or other software or hardware).
- Disable 'start automatically' for USB drives.
- Use HTTPS as your default (HTTPS Everywhere add-on for your Internet browser) and be alerted when visiting non-https websites (i.e., ordinary http:// instead of https://).
- Use Virtual Private Network (VPN) applications on computer and tablet/mobile when accessing public WiFi spaces (even if the WiFi has a password). This will secure your Internet connection and encrypt the data you are sending and receiving. Free versions include OpenVPN or CyberGhost.
- Use a digital signature to sign emails (like OpenPGP; see guide).
- Use encrypted tools and messengers like WhatsApp or Signal.
- Encrypt the content of your smart-phones (this can be done through the security settings on your phones, or by downloading software like PGP).

Stay secure with regular digital hygiene:

- Update your antivirus (software and virus definitions) automatically.
- Back up your data off-site – to the cloud or to an external hard-drive (connect it only when you back up, then disconnect); you can do it automatically or manually.
- Archive your data off-site – to the cloud or to an external hard-drive (backup is used for data recovery, while archiving is used for preserving and retrieving data in the event of a disaster, inquiry, or litigation. Back-up is short-term and archival is long-term – check the guide with best practices).
- Change your passwords occasionally (once every few months).
- Check and adjust your privacy settings on social media (companies update their policies regularly).

Visit our dedicated pages on Security issues for the latest developments.