Issue no. 10: April 2016 developments / Published on 30 April 2016

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

EMERGING TRENDS IN DIGITAL POLICY

We take a look at the past four months and observe key trends that have started to emerge: those related to the leading role that governments have been taking in cybersecurity matters, those that are bringing economic aspects closer to sustainable development, and those related to convergence and new technologies.

More on page 3

CYBERSECURITY

COMPETENCE BUILDING MEASURES

Cyberspace has become an essential component of modern society, yet its merits are accompanied by threats. A new study analyses the measures that ten OECD member states have applied to promote competence building in the field of cybersecurity.

More on pages 3, 8

ENCRYPTION

INTERVIEW WITH PHIL ZIMMERMANN

Developments in April show that more companies are switching on end-to-end encryption. The creator of Pretty Good Privacy, one of the most widely used encryption software, describes the evolution of encryption, the latest industry trends, and the legitimate interests of governments, users, and the industry.

More on page 6

PRIVACY

EU APPROVES NEW DATA PROTECTION RULES

The newly adopted General Data Protection Regulation harmonises rules across EU member states, and extends its scope to non-EU entities which process the personal data of EU residents. We describe the salient points and the main challenges.

More on page 7

TECHNICAL INNOVATION FOR DIGITAL POLICY

The conference on Technical Innovation for Digital Policy (Geneva, 25 April) brought together the technical community and policy-makers for a discussion on solutions to digital policy issues. From circumvention technology and cryptography, to next-generation secure architectures and open roots, technology offers the potential to tackle many issues. Advanced tools were described by their technical creators, while CyberLab demonstrations highlighted practical technical tools for user protection and how technology can also be used for illegal activity. Speakers included: Adrian Perrig from ETH Zurich (photo below), Louis Pouzin from Open Root, and Phil Zimmermann from Silent Circle. *Read the interview with Phil Zimmermann on page 6.*

(Photo: Aleksandra Virijevic)

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 at the Geneva Internet Platform premises | *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, Laetitia Honsberger, Aye Mya Nyein, Tereza Horejsova, Jovan Kurbalija, Aida Mahmutovic, Virginia Paque, Roxana Radu, Vladimir Radunovic, Barbara Rosen Jacobson, Emanuele Sacchetto, Sorina Teleanu | Send your comments to digitalwatch@diplomacy.edu. A Brazilian version in Portuguese is available at http://giplatform.org/newsletter

GENEVA DIGITAL DEVELOPMENTS

IGF Open Consultations and MAG meeting

Preparations for the 11th Internet Governance Forum (IGF),↗ which is scheduled to take place in Guadalajara, Mexico on 6-9 December, are now under way. The first round of open consultations, and a meeting of the Multistakeholder Advisory Group (MAG), ↗ which took place on 4-6 April, featured discussions on the programme and structure of the IGF 2016 meeting. The consultations also discussed the nature and content of IGF inter-sessional activities. It was decided that the overarching theme would be 'Enabling Inclusive and Sustainable Growth', while Internet and ICTs for the SDGs, human rights online, and critical Internet resources are some of the sub-themes. The consultations also agreed on the continuation of the work of the best practice forums (BPFs) on Internet Exchange Points and IPv6, and initiating new BPFs on cybersecurity, and gender and access; and strengthening interactions with national and regional IGF initiatives.

Cyber 9/12 Student Challenge

The Atlantic Council and Geneva Center for Security Policy hosted the Cyber 9/12 Challenge on 7-8 April.↗ More than 100 students and young professionals participated in a competition aimed at developing a response to a major cyber-attack on national level. Students were provided with a cyber-attack scenario described through intelligence reports, and were asked to analyse the threat it posed to state, military, and private sector interests, as well as to come up with responses to the political, economic, and security problems generated by the cyber-attack.

Cybersecurity Competence Building Trends

The study *Cybersecurity Competence Building Trends*, conducted by DiploFoundation and commissioned by the Swiss Federal Department of Foreign Affairs, was presented on 8 April ↗. The study outlines various measures that ten OECD member states applied to promote competence building in the field of cybersecurity. During the 8 April presentation, an overview of the main findings resulting from the study was given, and a discussion was held on the strategic, policy, and public private partnership approaches to cybersecurity capacity building. A follow-up webinar on 19 April ↗ discussed the main findings, and ways in which competence building measures can be integrated into national cybersecurity strategies. *Read more on page 3* *and page 8.*

Preventing Violent Extremism Online

How can terrorists and violent extremists be prevented from using the Internet? This was the underlying question of an expert meeting organised on 8 April during the Geneva Conference on Preventing Violent Extremism.↗ Most likely, the answer is close cooperation between the public and private sector. Panelists from both government and Internet companies (Facebook, Microsoft) highlighted the challenge in achieving a delicate balance between banning violent content and ensuring freedom of expression. The challenge is even more profound on an international level. As a concrete initiative, Europol announced the creation of an Advisory Group of experts that will help Europol develop a holistic approach to preventing violent extremism online.

Open Geneva Hackathon 2016

The Open Geneva Hackathon 2016 ↗, held from 16 to 18 April at Campus Biotech, brought together participants of various backgrounds, age, gender, and agendas, with the aim to develop solutions to global health challenges, by using geospatial data and other open data. The topics presented to the six teams competing in the hackathon included: urban navigation for people with visual impairment, forecasting emergencies, and online 'check-in'.

UNCTAD E-Commerce Week

The UNCTAD E-commerce Week ↗, held between 19 and 22 April, in Geneva, saw a variety of discussions on e-commerce and other related issues, such as privacy and data protection, cybersecurity, and digital trade regulation. The role of trust in maximising the digital economy was underlined throughout the week; enhancing both cybersecurity and users' privacy and data protection in the online space are key in this regard. The need for adequate and, to the extent possible, harmonised strategies, regulations, and policy frameworks in these areas, as well as for a strengthened cooperation between the various stakeholders (public bodies, private corporations, civil society organisations, etc.) was affirmed.

WIPO Conference on the Global Digital Content Market

The three-day WIPO conference on the global digital content market took place on 20-22 April. ↗ The discussion focused on the tension between increased access to content and a sustainable economic value chain, in particular copyright implications in the digital age; the role of publishers, producers, and distribution platforms; and digital markets, access, and participation. New technologies have changed completely how people produce music, films, and books, as well as how people purchase and share them. Many solutions were proposed to face the challenges discussed during the conference. First, we need regulation to be simpler even though the concept of IP is becoming more complex. Then there is the necessity of balancing access and sustainability of the industry. Finally, a clear regulation on the net neutrality issue is necessary to clarify the role of social media and Internet service providers (ISPs) in sharing content.

↗ Anytime you see this icon, there is more background material in the digital version. Alternatively, visit http://digitalwatch.giplatform.org for more in-depth information.

EDITORIAL

EMERGING TRENDS IN DIGITAL POLICY

In the last four months key trends have started to emerge in quite a few areas of digital policy. Our evaluation of such trends is supported by the rich interplay between data-mining and expert analysis. Among the most prominent trends are those related to intensive diplomacy around cybersecurity, those that are bringing economic aspects closer to sustainable development, and those related to convergence and new technologies.

This month, cybersecurity meetings between US and Russian officials took place; the trilateral summit between Russia, India, and China also had cybersecurity on the agenda. With legitimate interests to protect both their citizens and their country's economic interests and critical infrastructures, governments worldwide have been taking the lead in cybersecurity matters. Other bilateral agreements observed in previous months, as well as the growing interest in the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE), strengthen this trend. The effectiveness of governments' initiatives in cybersecurity will depend on the involvement of business, and user and technical communities, among others.

A second trend, particularly visible this month, can be seen from the concentration of e-commerce events which have served to bring economic considerations closer to sustainable development efforts. In particular, trade and development were among the underlying themes during UNCTAD's E-Commerce Week (18-22 April).

A third trend is the acceleration of ongoing tensions between the telecom and Internet industry, triggered by a shift in telecom services, from traditional ones to new over-the-top (OTT) services such as Voice over IP (VoIP). In Morocco, the decision of the country's National Telecommunications Regulatory Agency - that VoIP service providers did not have the necessary telecommunication licenses to operate – sparked outrage. The decision may affect users of WhatsApp, Skype, and Viber. This tension between the telecom and Internet industries is reflected in debates on net neutrality, consumer protection, and taxation, to name a few. Policy debates on how to find an optimal solution for both sectors are taking place in many forums worldwide, including within the ITU which is working on developing recommendations on OTT services.

RESEARCH

TRANSFORMING LABOUR MARKETS TO MEET CYBERSECURITY NEEDS

Cyberspace has become an essential component of modern society, yet its merits are accompanied by threats. The number of reported cyber-incidents has increased the need to build cybersecurity competences, especially for protecting the critical infrastructure.

The study *Cybersecurity Competence Building Trends,* conducted by DiploFoundation's researchers Vladimir Radunović and David Rüfenacht, analyses measures that ten OECD member states have applied to promote competence building in the field of cybersecurity. The study was commissioned by the Federal Department of Foreign Affairs of Switzerland.

The increasing dependence of the corporate sector on the Internet has also created a demand for qualified labour, which is being recognised by states as a possible driver for employment, economic growth, and global competitiveness. All the studied countries are developing the means to transform their national labour markets to meet this changing environment.

Eight dominant cybersecurity competence-building trends were identified in the study, and clustered within two categories:

- Measures for strengthening the academic programmes, with long-term effects.
- Measures related to professional training and knowledge frameworks, with shorter-term effects.

The first category includes measures such as: governmental support for university programmes; regional partnerships between research labs and multinational companies, aimed at increasing the country's or region's competitiveness in global cybersecurity markets; partnerships between universities and state security institutions; and university labelling programmes aimed to better correlate the curricula with the needs of public institutions.

One key trend in the second category is the collaboration between public institutions and professional certification bodies, leading to a soft standardisation of the minimum knowledge and ability requirements for cybersecurity personnel.

Other trends include: measures to improve the competences of the private sector, especially small and medium enterprises and operators of critical infrastructure; cybersecurity training for decision-makers, managers, and senior executives; as well as the development of cybersecurity-related job descriptions, and the definition of the required knowledge training for such jobs.

The study concludes by saying that the identified trends lead not only to the development of national competences for responses to cyber-threats, but also to the consolidation of cutting-edge cyber-industries that increase the competitiveness of states in the global cyber-markets.

An executive summary is also available, while illustrations from the report are included on page 8 of this newsletter. Visit the cybersecurity page on the GIP Digital Watch observatory for additional resources, instruments, upcoming events, and more.

CYBERSECURITY COMPETENCE BUILDING TRENDS

Research report
Commissioned by the Federal Department of Foreign Affairs of Switzerland

Vladimir Radunović and David Rüfenacht
DiploFoundation
February 2016

DiPLO
www.diplomacy.edu

DEVELOPMENTS IN APRIL

Global IG Architecture

same relevance

A Joint Communiqué of the G7 Foreign Ministers expresses concern over threats posed by terrorists' use of the Internet and social networks. It reconfirms that existing international law applies to cyberspace, and reaffirms the commitment to a multistakeholder approach to Internet governance.

The 11th Internet Governance Forum meeting, in Guadalajara, Mexico, is scheduled for 6-9 December.

Sustainable development

same relevance

G7 Foreign Ministers commit to 'utilizing ICTs in addressing global issues and achieving progress on the 2030 Agenda for Sustainable Development'.

Online discussions on science, technology, and innovation for sustainable development goals (SDGs) are ongoing among stakeholders; discussions will feed into the first multistakeholder forum on science, technology, and innovation for the SDGs (New York, 6-7 June).

Security

increasing relevance

Further high-level discussions take place on cybersecurity: Senior US and Russian officials renew efforts to prevent the countries from mistakenly attributing attacks to each other. Russia, India, and China reaffirm the UN's key role in addressing issues of security in the use of ICTs and support the adoption of universal rules on state behaviour.

The Panama Papers leak wreaks havoc among many governments; the breach exploits a common website vulnerability.

Mobile apps and Internet services - including WhatsApp, Viber, and Wordpress - switch on encryption.

Privacy and human rights

increasing relevance

The EU's data protection advisory group - Article 29 Working Party - expresses concerns over the complexity of the new EU-US Privacy Shield, and the public authorities' access to data transferred under the framework. *More on page 7.*

The European Union adopts the General Data Protection Regulation, which allows for more user control of data, including the right to request the erasure of personal data, and provides for the right to data portability, among other features. The main challenge relates to its implementation. *More on page 7.*

The Council of Europe's Committee of Ministers adopts a Recommendation on Internet Freedom, declaring that the European Convention on Human Rights applies both offline and online.

UNCTAD's report on Data Protection Regulations and International Data Flows suggests that a 'core set' of data protection principles can serve as a useful starting point for more compatibility and harmonisation. It identifies seven areas where action is needed, and offers policy options for national, regional, and international initiatives.

The 2016 World Press Freedom Index, by Reporters Without Borders, reveals a 'deep and disturbing decline in respect for media freedom'.

Infrastructure

same relevance

The European Commission launches the European Cloud Initiative as part of a wider package of measures for digitising European industry. The initiative envisions the creation of a European Open Science Cloud and the deployment of a European Data Infrastructure.

The telecom regulatory authority in Morocco is sued for blocking VoIP services.

A report from security company Trustwave confirms that spam volumes continue to decrease.

Net neutrality

same relevance

The White House has threatened to veto the passage of an anti-net-neutrality bill (Rate Regulation of Broadband Internet Access Act), which could remove the US Federal Communications Commission's authority to set broadband rates or review whether a rate is reasonable. Earlier, the House of Representatives voted in favour of the bill.

Egypt's decision to block Facebook's Internet.org came after the company refused to accede to surveillance requests, Reuters reveals.

E-commerce and Internet economy

same relevance

Google has breached the EU antitrust rules, according to the European Commission. Google 'abused its dominant position by imposing restrictions on Android device manufacturers and mobile network operators'.

Data protection, e-trade, and measuring e-commerce are the focus of UNCTAD's E-Commerce Week, with the launch of the Data Protection Report (above), and the B2C E-Commerce Index (2016). The sustainability of emerging economic models of the digital content was the focus of the WIPO Conference on the Global Digital Content Market.

Jurisdiction and legal issues

same relevance

The EU's new GDPR expands its territorial reach to non-EU entities processing the personal data of Europeans. In addition, where a company has multiple establishments in different EU countries, it will fall under the responsibility of a lead authority (one-stop shop) in the country of the company's main establishment. *More on page 7.*

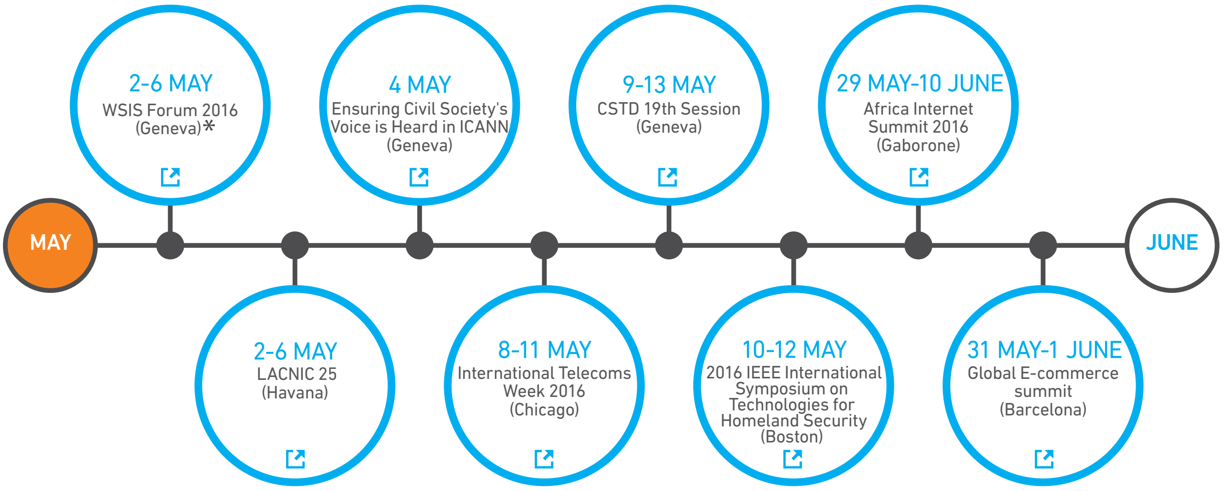
IANA Transition

same relevance

ICANN and Verisign will run a parallel test of the root zone management system. The test, which will run for 90 days, is intended to verify the integrity of the data contained in the root zone file following the transition of the IANA functions stewardship.

ICANN launched a public comment period on the draft of its new bylaws. The new bylaws reflect changes resulting from recommendations contained in the IANA stewardship transition proposal and in the accountability proposal.

AHEAD IN MAY



MAY

2-6 MAY
WSIS Forum 2016
(Geneva)*

2-6 MAY
LACNIC 25
(Havana)

4 MAY
Ensuring Civil Society's Voice is Heard in ICANN
(Geneva)

8-11 MAY
International Telecoms Week 2016
(Chicago)

9-13 MAY
CSTD 19th Session
(Geneva)

10-12 MAY
2016 IEEE International Symposium on Technologies for Homeland Security
(Boston)

29 MAY-10 JUNE
Africa Internet Summit 2016
(Gaborone)

31 MAY-1 JUNE
Global E-commerce summit
(Barcelona)

JUNE

***The *GIP Digital Watch* observatory will feature live updates and reports during the WSIS Forum 2016. Visit the dedicated webpage**

INTERVIEW

ENCRYPTION: AN INTERNET NECESSITY

The recent Apple/FBI controversy has contributed to heightened awareness of privacy, security, and encryption. In its aftermath, more companies are now switching on end-to-end encryption. In an interview for the *GIP Digital Watch* newsletter, PHIL ZIMMERMANN describes the evolution of encryption, the recent industry trends, and the legitimate interests of governments, users, and the industry.

When it comes to cryptography, Phil Zimmermann needs no introduction. He is the creator of Pretty Good Privacy (PGP), a widely used encryption software, and a founder of Silent Circle, a Geneva-based privacy communication company. With over 30 years of industry experience, his analysis of the evolution of encryption goes back to when the legislative environment looked at encryption in a much different way than it does today.

'In the 1990s, if you were using strong encryption, you had to explain yourself. You had to defend it. Today, if you are not using strong encryption, you have to defend yourself.'

A medical clinic that does not encrypt patient records or a business executive who carries unencrypted customer data on his/her laptop run the risk of reputational damage if the data are breached. In some legislation, this can result in civil liability and penalties, possibly even criminal sanctions. Public statements, necessary in certain scenarios, can also be quite damaging. This is a big change from the environment in the 1990s.

Zimmermann explains that at the time, there was hardly any good encryption. While governments were able to encrypt communications, it was very difficult for ordinary people to communicate securely.

'No method of encrypted long-distance communications existed for normal people. Whatever rudimentary encryption existed at the time, it was not sufficient. Pretty Good Privacy changed this. I wanted to see the software used by grassroots political organisations and human rights groups.' Attracted by the fact that the Swiss constitution grants the right to privacy, Silent Circle's company executives eventually moved the company's headquarters to Geneva.

(Photo: Aleksandra Virijevic)

While there are many encryption tools for which users do not require technical knowledge, PGP requires an understanding of cryptography keys, certificates, and trust models. Despite the popularity of certain software, Zimmermann believes that the need for technical expertise is why large-scale e-mail encryption has not taken off.

Yet, things may have started to change. More industry players are switching on end-to-end encryption and offering secure communications to their users. WhatsApp is one such example. According to Zimmermann, the fact that the company has switched on encryption for its billion users at the same time is a tremendously significant event. It is one of the defining moments in the evolution of cryptography, together with the change which PGP brought about, and the introduction of the security standard Secure Sockets Layer (SSL) into web browsers and other products.

This shift comes in the aftermath of the Apple/FBI controversy, which brought encryption, privacy, and security into focus. The controversy also highlighted the legitimate interests of the main players and the interplay between law enforcement and industry.

Apple has helped the FBI a number of times, where it could. But Zimmermann believes that there are other ways of obtaining evidence, including forensic analysis, physical evidence, and transactional information. While law enforcement does have a legitimate interest, Zimmerman reckons that 'putting a back door in encryption means putting a back door that can be exploited by bad guys,' as that would have compromised the integrity of a product for everyone, and not for that one particular case.

'Many cryptographers have tried hard to find ways to create a backdoor that is available only for good guys, but nobody has come up with a way to do that. I think it's impossible. If you want security, you need to have privacy. Privacy-enabling technology improves security. These are not mutually exclusive. In fact, one is required for the other.'

Zimmermann hopes that the shift in favour of stronger encryption will be a market differentiator. He hopes the trends will create market incentives and will encourage users to recognise the importance of encryption. We will keep an eye on the trends.

Phil Zimmermann was a speaker at the Geneva Internet Platform's conference on Technical Innovation for Digital Policy, on 25 April. The conference was organised in cooperation with the University of Geneva, ETH, and DiploFoundation. Read the event report.

> *'Putting a back door in encryption means putting a back door that can be exploited by bad guys.'*

EU APPROVES NEW DATA PROTECTION RULES

The European Union has just adopted the long-awaited General Data Protection Regulation (GDPR). After four years of negotiations, the rules will become applicable in 2018. The GDPR, formally adopted by the Council of the EU (on 8 April) and the European Parliament (on 14 April), harmonises data protection rules across EU member states, and extends its scope to non-EU companies. In this article we describe the salient points and the main challenges.

The salient points

Expanding territorial reach: The GDPR will now also apply to non-EU companies that offer goods or services to Europeans, or monitor their behaviour (such as tracking users' online behaviour or preferences).

Harmonisation: The GDPR aims to harmonise the rules related to data protection across all member states, making it easier for EU and non-EU companies with multiple establishments across Europe to comply with the regulation.

A one-stop shop: Although not as envisaged in earlier drafts of the GDPR, the concept of a one-stop shop is aimed at facilitating the operations of companies across the EU. Member states will now be required to establish independent Supervisory Authorities (SAs), which will supervise the data processing activities of companies handling personal data, and will provide mutual assistance to other SAs. They will also hear and investigate complaints. Companies with multiple establishments will fall under the lead authority in the country where their main data processing activities take place.

Data protection by design and by default: Companies operating in the EU must set default privacy settings for their products and services to high, and must ensure that data protection rights are taken into account when developing processes for data handling.

Notice requirements: Companies must now specify the retention time of personal data in their notices to users. Other policies and impact assessments will be imposed on companies.

Right to erasure: Under this right, which is more limited than the right to be forgotten (also included in the GDPR), users can request the erasure of personal data on a number of grounds. Users can also request access to their data and have the right to object to the processing of their data in certain situations.

Explicit consent: A user's explicit consent for the processing of personal data will be required when the data are particularly sensitive and vulnerable in relation to privacy and other fundamental rights.

Data portability: The right to data portability enables users to obtain a copy of the personal data undergoing processing. The GDPR requires companies to provide such data in an electronic and commonly used format.

Children's consent: When it comes to processing the data of a child, the GDPR requires the consent of a parent or guardian where services are addressed directly to children under the age of 16 – or a lower age (not below 13) if this is set by member states.

In addition, the Article 29 Working Party (WP29; composed of representatives of national Data Protection Supervisory Authorities, the European Data Protection Supervisor, and the European Commission) will be replaced by the European Data Protection Board, which will coordinate the SAs.

The challenges

The biggest challenge will be the implementation of the GDPR, as companies handling personal data of EU residents must adopt new working methods and transform their business practices in line with the GDPR.

The provisions of data portability will be particularly challenging to implement; one of the main questions is whether companies will have sufficient facilities to comply with a user's request with regard to all data falling under the scope of this provision.

A high standard of data protection has to be agreed by all European data protection authorities; different interpretations of the GDPR may therefore still lead to different levels of privacy protection.

EU-US PRIVACY SHIELD AWAITS APPROVAL

After months of legal uncertainty, the EU-US Privacy Shield ↗ is materialising. The new agreement for transatlantic data flows will replace the Safe Harbour agreement, which was invalidated last year by the Court of Justice of the EU, in the Max Schrems judgment.↗

The agreement, a result of challenging negotiations between EU and US officials, was released in February. The framework will impose stronger obligations on US companies to protect the personal data of Europeans. It will include several redress possibilities and will require additional supervision by the US Department of Commerce and the Federal Trade Commission. The framework also foresees an annual joint review mechanism.

In an opinion issued on 13 April,↗ WP29 expressed its serious concerns over the lack of clarity of the framework, and the fact that key principles under EU law are not reflected therein. It was also concerned with the lack of sufficient independence of the Ombudsman – a new redress mechanism in the framework. It has asked the Commission to resolve these concerns.

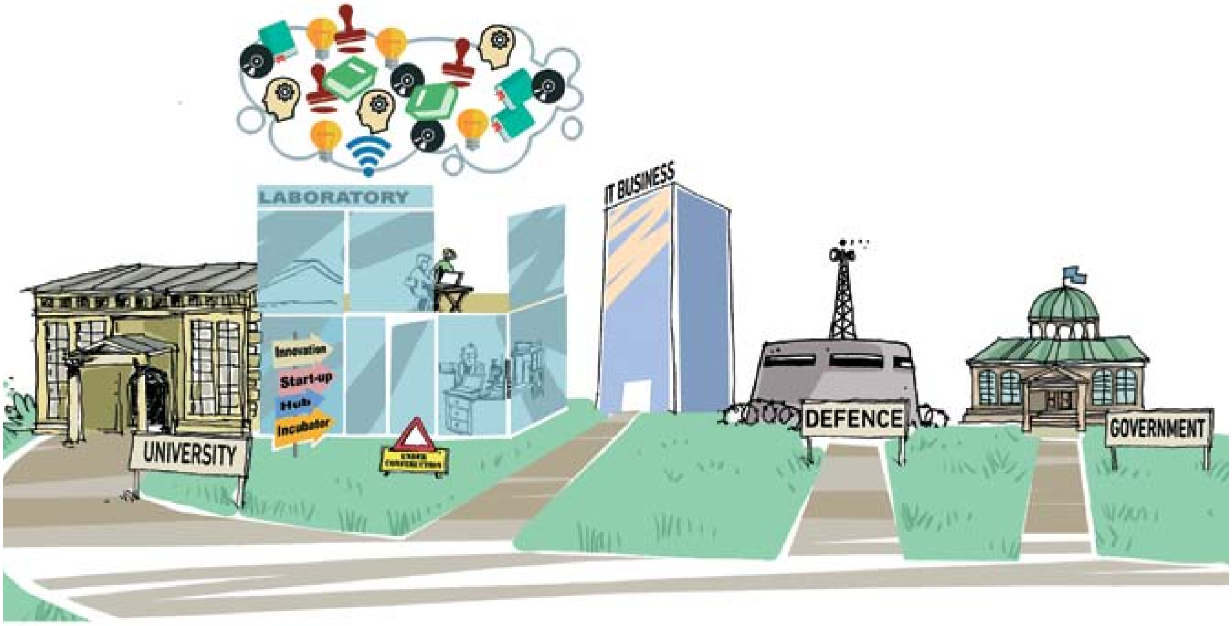
It is very likely that the Privacy Shield will undergo further changes with time. Not only is this due to the anticipated annual review by EU and US officials, as indicated in the framework itself, but also because WP29 has indicated the need for a review of the framework after entry into force of the GPDR in 2018.

KEY CYBERSECURITY COMPETENCE BUILDING TRENDS

The study *Cybersecurity Competence Building Trends,* conducted by DiploFoundation's researchers, identifies eight dominant cybersecurity competence building trends. Each of the trends are described in detail, and illustrated. Here, we reproduce two of the illustrations and the corresponding trends. *Read more about the study on page 3 of this issue.*

UNIVERSITY
FUEL
Knowledge
Research
Idea
Co.
Gov
CYBER-CHALLENGES

Long-term effects on cybersecurity are enabled by strengthening university curricula and research capacities through financial support by the public and private sectors. All of the OECD countries explored are actively supporting the development of university and research programmes.



Developing a cybersecurity industry through innovation hubs and joint ventures attached to established universities strengthens national competences and competitiveness on the global market. Most of the larger research labs in OECD countries have partnered with multinational companies. Such partnerships provide funds and conditions to enhance the academic portfolio, develop cutting-edge and applied solutions to technology, and increase the global competitiveness of the region and the country in cybersecurity markets.