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.

DIGITAL POLICY TRENDS IN NOVEMBER

1. The search for cyber-norms continues

After the fifth meeting of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) ended without consensus, the search for ways and means to address cybersecurity issues on a global level continues.

In Geneva, Microsoft's President renewed his call for a Digital Geneva Convention as a way to make governments responsible for cybersecurity. In parallel, the Geneva Digital Talks addressed technical solutions to the growing cybersecurity challenges. While there are many political aspects in the cybersecurity debate, technical solutions could fix some of the major cybersecurity problems. *More on page 2.*

In New Delhi, the Global Conference on Cyberspace covered some aspects of global cybersecurity cooperation, especially when it comes to capacity development. At the same meeting, the Global Commission on the Stability of Cyberspace (GCSC) issued a Call to Protect the Public Core of the Internet, urging state and non-state actors to avoid activity that would intentionally and substantially damage the general availability or integrity of the 'public core' of the Internet. It remains to be seen how the major actors in the cyber field will react to this call.

The main question is where and how governments will converge again towards adopting global solutions for cybersecurity.

2. Debate on lethal autonomous weapons unfolds

The debate on lethal autonomous weapons systems (LAWS) continued this month with a week-long high-level discussion in Geneva. The newly formed Group of Governmental Experts (GGE), under the framework of the Convention on Certain Conventional Weapons, reached various conclusions after a discussion with leading experts.

The group took a realistic approach to the development of LAWS, concluding that the technology should neither be hyped nor underestimated. While acknowledging that fully autonomous weapons systems have not yet been developed, how can the risks related to LAWS be mitigated? The GGE's discussion pointed to several solutions.

Continued on page 3

Bitcoin surged past USD$11 000 per unit on Wednesday, 29th November, hours after it crossed USD$10 000. *More digital policy developments on pages 4–5.*

IN THIS ISSUE

Issue no. 26 of the *Geneva Digital Watch* newsletter, published on 30 November 2017, by the Geneva Internet Platform (GIP) and DiploFoundation | Contributors: Stephanie Borg Psaila, Jovan Kurbalija, Virginia Paque, Roxana Radu, Barbara Rosen Jacobson, Sorina Teleanu | Design by Viktor Mijatović, layout by Aleksandar Nedeljkov, Diplo's CreativeLab | In addition to the newsletter, you can find in-depth coverage of developments on the *GIP Digital Watch* observatory (http://dig.watch) and join discussions on the last Tuesday of every month online, or at the GIP (http://dig.watch/briefings) | Send your comments to digitalwatch@diplomacy.edu

GENEVA DIGITAL DEVELOPMENTS

How Can Technological Solutions Advance Cybersecurity?

The second session of the Geneva Digital Talks, held on 3 November, discussed how cybersecurity as a field interacts with recent or potential technological changes. The panel debate highlighted the dichotomy between technology and policy in the cybersecurity domain and the need to enhance trust and collaboration between the two fields. On the technological side, one practical solution was presented: The Scalability, Control, and Isolation on Next-Generation Networks (SCION) architecture, developed by a team at ETH Zurich, allows individuals to control the pathways through which their data travel, while providing an additional layer of security by ensuring fuller control of their networks.

Geneva Peace Week 2017

Throughout the 2017 edition of the Geneva Peace Week, held on 6–10 November, it became clearer that digital technology has important implications for conflict prevention, albeit in two distinct and contradictory ways. Some sessions identified the ways in which digital technology can assist in the prevention of conflict. They highlighted the potential of e-commerce, big data, AI, and geographic information systems. At the other end of the spectrum, there was a focus on the ways in which digital technologies have given rise to increased threats.

Preventing Cyber Conflicts: Do We Need a Cyber Treaty?

The third session of the Geneva Digital Talks, on 9 November, built on Microsoft's president Brad Smith's call for a Digital Geneva Convention, and developed around three main considerations. First, it was considered that addressing cybersecurity challenges requires a mentality shift: 'Peace cannot be indoctrinated but it needs to be discussed as a mentality, as a climate.' Second, speakers stressed the importance of a multistakeholder approach to the drafting of a possible cyber treaty (for example, the Montreux process). Finally, it was noted that Microsoft's proposal is a welcome call for governments to take action to address vulnerabilities in cyberspace.

Big Data for Prevention: Balancing Opportunities with Challenges

Held as part of the Geneva Peace Week 2017, this session explored the potential of big data for conflict prevention. The discussions underlined that technology can constitute both a risk of inciting conflict and a mitigation factor, and that data may have multiple interpretations and facets. Visualisations (such as the tool developed by the UN Interregional Crime and Justice Research Institute (UNICRI) and CERN) play a key role in helping analysis and provision of knowledge-based data. Satellite data was given as an example of big data that can contribute to conflict prevention, by reporting and documenting early warning indicators, while providing actionable information for the national and international communities.

Current Internet Governance Challenges: What's Next?

This event, held on 9 November, featured discussions on current Internet governance challenges and possible ways of addressing them. Despite the benefits brought by the Internet, more than 3.5 billion people remain unconnected. The risk of conflict and a new arms race involving cyber weapons, and online terrorist propaganda and extremist violence were identified as growing challenges, which require political will when it comes to identifying solutions. The focus of the discussions was on cybersecurity and the need to look at it as a shared responsibility. In this regard, Microsoft's president Brad Smith reiterated the proposal for a tech sector accord in the field of cybersecurity, and a Digital Geneva Convention to guide the behaviour of governments in cyberspace.

Sharing Economy and its Social Challenges

This high-level discussion, on 21 November, focused on the way digital platforms work and how to determine whether they empower or exploit their workers. The new business models for the sharing economy rely on the network effect: a company no longer creates the end product or service; it provides a common infrastructure and matches consumers and producers using the knowledge of the market. The speakers agreed that the social function of work should be in focus and that solutions need to be people-centred.

6th United Nations Forum on Business and Human Rights

Held on 27–29 November under the theme 'Realising access to effective remedy', the Forum featured over 60 sessions dealing with business-related human rights issues. Discussions emphasised that while technology is vital to modern society, technological developments have increased concerns regarding the protection of human rights, such as privacy and freedom of expression. New forms of human rights abuse in the digital age could be avoided if stakeholders – companies, governments, and civil society – work together on identifying and implementing tools for human rights protection and enforcement.

Where and How to Protect Legal Interests in the Digital Era

In this session, held on 28 November, as part of the Geneva Digital Talks, three panellists offered answers from different perspectives to the question of what, if at all, is the role of courts in Internet governance and how access to justice can be ensured in the online space. The discussion reflected on regulations of traditional Internet governance matters, contrasting them with present technological issues. Digital policy and the practice of arbitration are both leveraging the position of Geneva as a major global hub for solutions.

This icon indicates that there is more background material in the digital version. Alternatively, visit http://dig.watch for more in-depth information.

DIGITAL POLICY TRENDS IN NOVEMBER

Continued from page 1

Conducting national legal weapons reviews is required under Additional Protocol I to the Geneva Conventions. This is considered a safeguard to ensure the compliance of newly developed weapons with international humanitarian law. Yet, some states argue that national reviews are not sufficient.

Developing policy options could include a legal instrument, such as an additional protocol, prohibiting LAWS; a politically binding declaration; or a future Code of Conduct. Experts also mentioned the need for an immediate moratorium on the deployment of LAWS. Some argued, however, that a ban is premature, as such weapons have not yet been developed.

Risk-mitigation could also be further integrated into the design. The industry is working to address risks, 'including through robust validation and verification as well as testing and evaluation methodologies. Some are integrating ethics into design and development and looking at best practices from around the world.' States could encourage this practice further.

Additional analysis on the key issues that emerged during the discussions is on page 7.

3. Failure to disclose: More leaks and vulnerabilities

Uber is in hot water again, this time over a data leak it failed to disclose. After the company's servers were breached in 2016, Uber paid $100,000 to the intruders to delete the data and keep silent, Bloomberg revealed. Criminals accessed the names, e-mail addresses, and phone numbers of over 50 million Uber riders, as well as the personal information of about 7 million drivers.

The question is: Are companies obliged to disclose data breaches? The legal framework in the USA obliges companies to alert the public and government agencies. When it comes to the data of European citizens, the EU's General Data Protection Regulation, which is due to take effect in May 2018, will also oblige companies to report breaches promptly.

Conversely, vulnerabilities discovered by governments also need to be disclosed. In November, the US White House released an updated version of its Vulnerability Equity Process (VEP), according to which US security agencies decide which of the vulnerabilities they have discovered will be disclosed to the software's developer, and which will be withheld. The government discloses more than 90% of the vulnerabilities it finds.

What about the rest? Non-disclosed vulnerabilities could be leaked and again cause global havoc, as the WannaCry ransomware did. Whistleblower Edward Snowden has also warned that nondisclosure of 10 significant security flaws outweighs the benefits of disclosing 90 low-severity flaws.

4. Courts shaping digital policy; complexities arise

Once again, courts continue to shape the applicability of digital policy across different jurisdictions, adding to the complexities in the process.

This month, a US judge blocked a decision by Canada's Supreme Court from being applicable in the USA. In June, the Canadian Supreme Court had ordered Google to remove search results that violated intellectual property rights worldwide, and not only within Canada.

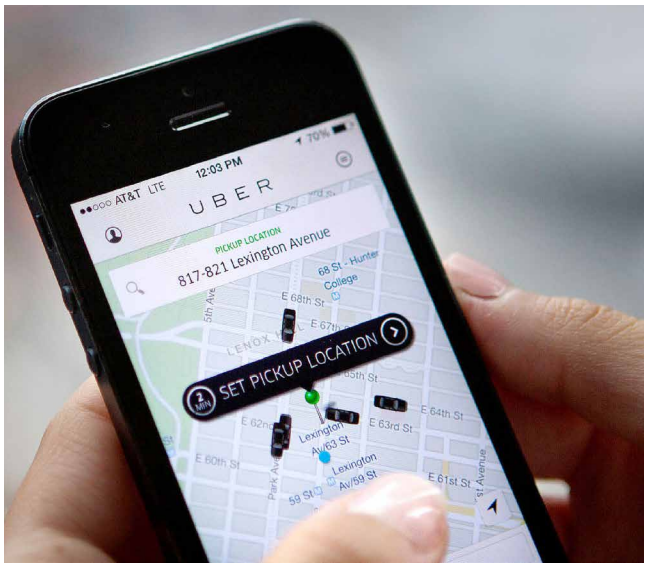
This is not the first time that courts have issued conflicting rulings. An appeals court ruled that the government could not use a search warrant to force Microsoft to turn over data stored in Dublin, but a Philadelphia court ruled that Google must comply with FBI search warrants (the data in Google's case was considered a 'moving target'). Uber-related cases offer another example: While some courts have ruled that Uber drivers are independent contractors, other courts have ruled that the drivers are employees. As one expert notes, court decisions can sometimes give rise to conflicting rulings.

5. Rifts visible in e-commerce negotiations ahead of MC11

Ahead of the World Trade Organization (WTO) Ministerial Conference (MC11) next month, rifts are already appearing between developing and developed countries. As we noted last month, digital policy issues are increasingly framed as trade-related issues, and whereas some countries are in favour of negotiating new e-commerce rules at MC11, others are against this.

In continuing debates, a large majority of developing countries, including India and South Africa, have made it clear they will oppose negotiations. At the meeting, convened by the General Council Chair on 21 November, these countries said they will adhere only to the existing non-binding 1998 work programme. The European Union, along with Japan and other developed countries, are arguing in favour of advancing an e-commerce agenda. Addressing newer trade-related aspects would increase their uptake online, the EU believes.

MC11 will take place on 10–13 December in Buenos Aires. Follow the GIP Digital Watch observatory for updates.



After Uber's servers were breached in 2016, the company paid the intruders to delete the data and keep silent.

DIGITAL POLICY: DEVELOPMENTS IN NOVEMBER

Global IG architecture

increasing relevance

After the UN GGE meeting ended without consensus, the search for venues to address some cyber-security issues continues. *More on page 1.*

Sustainable development

same relevance

The ITU has announced an increase in its indicators, used to assess and rank ICT development across countries. The new methodology of 14 indicators, instead of 11, is designed to capture recent developments in ICT markets, with the introduction of emerging technologies. The ICT Development Index is a core feature of the ITU's annual *Measuring the Information Society Report*.

Security

increasing relevance

The number of distributed denial of service (DDoS) attacks continues to increase as criminals take advantage of insecure IoT devices. A report by Corero Network Security reveals a 35% increase in monthly attack attempts compared to the previous quarter, and a 91% increase in monthly attack attempts compared to the first quarter of 2017.

A security vulnerability in Ethereum wallets froze 500 000 units of the Ether cryptocurrency. This occurred to multi-signature wallets, i.e., wallets which require more than one owner to 'sign' a transaction. Parity Technologies, the company behind the wallets, said that this occurred due to an accidental global exploitation of a vulnerability, which permanently locked more than USD$150 million in cryptocurrency.

E-commerce & Internet economy

increasing relevance

Bitcoin surged past USD$11 000 per unit, hours after it crossed USD$10 000. The proposed SegWit2X upgrade of the Bitcoin payment system, known as the New York Agreement, has been postponed. The upgrade failed to gain the widespread support needed among Bitcoin users. On a global level, the WTO's Ministerial Meeting is not likely to reach consensus on advancing the e-commerce agenda. *More on page 3.*

At regional level, shifts in the dynamism of e-commerce were noted. Trade ministers from the 11 remaining Trans-Pacific Partnership (TPP) countries announced they agreed on the core elements of the deal. Nevertheless, a planned meeting to announce the deal was cancelled after the Canadian Prime Minister decided not to attend, due to some remaining concerns. Negotiators from Canada, Mexico, and the USA concluded their fifth round of talks to modernise the North American Free Trade Agreement (NAFTA). The negotiations made substantial advances in sectors such as telecommunications, trade facilitation, e-commerce, and technical barriers to trade.

The UK Treasury is preparing for unilateral action on taxing the digital economy. It will push for international tax reforms, while exploring interim solutions to raise revenue from digital businesses. Uber is facing more legal woes. In the UK, the ride-sharing company has lost its appeal against a court ruling issued last year by an employment tribunal, which ruled that Uber employees are workers entitled to minimum-wage rights. The company plans to continue to challenge the decision. Uber drivers in Nigeria have initiated a similar case in a Lagos court.

Digital rights

increasing relevance

Uber covered up the leak of the data of 57 million users, Bloomberg reports. *More on page 3.* In the UK, Google is taken to court over allegations that it has ilegally collected personal data of over 5 million users by bypassing privacy settings of their iPhones.

Venezuela's Constituent Assembly has passed a law its authors say 'would punish messages of hate in broadcast and social media with penalties reaching 20 years in prison'.

The Council of Europe (CoE) and Russian antivirus software developer Kaspersky Lab, as well as other IT and Internet companies, have pledged to protect human rights and help maintain a secure Internet. They will cooperate on combatting child online sexual exploitation and abuse; countering cybercrime and terrorism; and promoting human rights online.

Internet freedom has declined for the seventh consecutive year, Freedom House's *Freedom on the Net 2017* reveals. The use of social media to 'advance an anti-democratic agenda' has brought new challenges, as it is 'more difficult to combat than other types of censorship', the project's director explained.

Jurisdiction & legal issues

increasing relevance

A California judge has blocked the Canadian Supreme Court's right to be forgotten ruling from taking effect in the USA. *More on page 1.*

The European Commission is setting up a High-Level Expert Group on fake news and online disinformation, with representatives of academia, the tech industry, news media, and civil society. It has launched a public consultation to feed into an EU strategy on how to tackle the spread of fake news.

Infrastructure

same relevance

A new law in Russia restricting the use of proxy tools such as virtual private networks (VPNs) and anonymisers, came into force on 1 November.

Russia's Security Council has reportedly instructed the government to start talks among BRICS countries (Brazil, Russia, India, China and South Africa) about the possibility to build an alternative DNS root server system.

Microsoft-owned Skype has been removed from several Chinese app stores, including those operated by Apple and Android. Apple was notified by the Ministry of Public Security that 'a number of voice over Internet protocol apps do not comply with local law.'

Net neutrality

increasing relevance

The US Federal Communications Commission (FCC) is preparing to vote on rolling back the 2015 net neutrality rules. *More on page 6.*

The Telecom Regulatory Authority of India released a set of recommendations in support of net neutrality, noting that licensing terms applicable to Internet service providers (ISPs) should include explicit restrictions on any sort of discrimination in Internet access based on content accessed, protocols used, or equipment deployed.

New technologies (IoT, AI, etc.)

increasing relevance

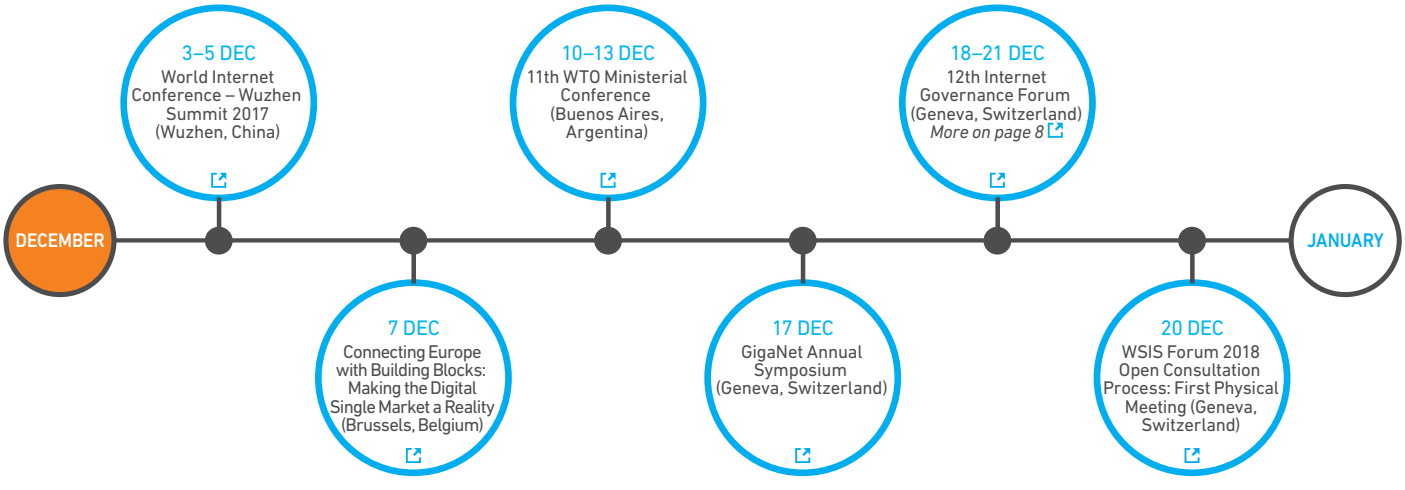
The GGE on LAWS met for the first time in Geneva, to discuss the technological, military, legal, and ethical issues surrounding LAWS. *More on pages 1 and 7.*

In Tokyo, chatbot Shibuya Mirai – programmed to resemble a 7-year-old boy – was granted official residence. The chatbot is aimed at making the local government more familiar and accessible to residents, allowing officials to hear their opinions.

In Arizona, USA, the Alphabet-owned company Waymo has started testing self-driving cars on public roads, without a human safety driver on board. The UK announced plans for fully self-driving cars, without a human operator, by 2021. Singapore aims to have driverless buses by 2022.

A report published by the Centre for Policy Studies in the UK argues that taxing robots will not protect jobs, and that calls for a universal basic income are premature, as this would distort the labour market.

AHEAD IN DECEMBER



For more information on upcoming events, visit http://dig.watch/events

NET NEUTRALITY IN TURMOIL

The US FCC is expected to roll back rules supporting net neutrality in December. The 2015 rules were strongly in favour of net neutrality. Will the new rules undermine protection for net neutrality principles?

Earlier this year, the US FCC announced its intention to roll back these rules. This campaign was spearheaded by chairman Ajit Pai. The Republican-majority FCC is now expected to vote in December to replace the 2015 Open Internet Order with the new Restoring Internet Freedom Order.

The 2015 rules were strongly in favour of net neutrality. They reclassified broadband Internet access service providers as so-called utility carriers, which meant that they were subject to the FCC's authority and oversight to ensure that they do not interfere with the speed or selection of content through the Internet access they provide to their users.

The new draft rules, circulated in November, would restore the classification of broadband providers as 'information service' providers, thus limiting the FCC's authority over them, and allowing them to develop models that run counter to net neutrality principles. The new rules would only require that ISPs be transparent and disclose information about their practices to consumers, entrepreneurs, and the commission.

Mixed reactions

The draft rules have found support from companies such as Verizon and Comcast, which have also asked the FCC to pass a ruling confirming the primacy of federal law, and preventing individual states from adopting their own net neutrality regulations, once the new order is in place.

However, other Internet companies are opposing the new plans. Among these are Google, Facebook, and Netflix; they believe that the current rules are working well. Another 200 technology companies, among them AirBnB, Reddit, and Twitter, share this view and have sent a letter to the FCC asking that the commission vote against the new regulations.

Beyond US shores, one reaction came from Canada, where Prime Minister Justin Trudeau has expressed concerns over the possible rollback of net neutrality rules in the USA, noting that net neutrality 'is essential for small businesses, for consumers, and it is essential to keep the freedom associated with the Internet alive'.

While most eyes are on the USA, India has also attracted attention recently, as its Telecom Regulatory Authority released a set of recommendations in support of net neutrality.

What will happen next?

With only few weeks left before the FCC vote, there are several possible scenarios:

1. **Activism**. In July this year, major Internet companies and civil society organisationts took part in a massive online 'day of action' in support of net neutrality rules, as part of the *Battle for the Net* campaign. The campaign has now been relaunched, and activists across the USA plan a protest on 7 December. It remains to be seen whether such actions will have the desired impact.

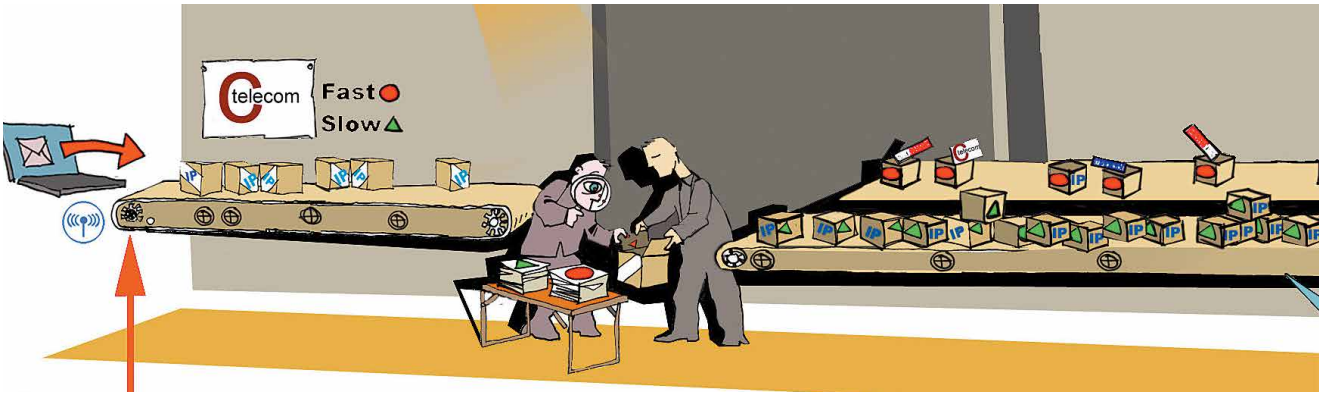
2. **Congress**. In an interview in September, FCC Chairman Pai spoke in favour of the net neutrality issue being tackled by the US Congress, which 'would be well-positioned to take hold if this issue and just figure out what the rules or the road are going to be long term'.

This might be case, as there are several voices calling for Congress to step in and start working on legislation in support of net neutrality. But there is also the possibility – at least in theory – for Congress to pass a Congressional Resolution of Disapproval, and discard the FCC's repeal of the 2015 Open Internet order. The likelihood of either of these two options becoming a reality is uncertain.

3. **Court action**. If the FCC passes the order proposed by Chairman Pai, it is possible that this will be attacked in court, based on the reasoning that it is not duly justified. In line with US jurisprudence, agencies cannot reverse existing rules without offering solid argumentation:

A Supreme Court decision issued in 1983 stated that 'an agency changing its course by rescinding a rule is obligated to supply a reasoned analysis for the change beyond that which may be required when an agency does not act in the first instance.' Commentators argue that this is not the case with the proposed order, which seems to be based on the argument that investments in broadband infrastructures have dropped over the past two years.

Follow the GIP Digital Watch observatory for updates.



LETHAL AUTONOMOUS WEAPONS SYSTEM: EXPERTS MAP MAIN ISSUES

Technology has always revolutionised conflict. Yet today, society might be on the brink of an existentially different technological development: the loss of human control in warfare. In November, the GGE explored technological, military, legal, and ethical implications related to such systems.

To avoid scenarios in which LAWS cause unnecessary harm, the High Contracting Parties to the Convention on Certain Conventional Weapons (CCW) established the GGE to examine issues related to emerging technologies in the area of LAWS, with the involvement of different stakeholders. During the group's discussions, on 13–17 November, five key issues emerged.

1. Predictability and reliability: Can we trust a killer robot?

While perfectly autonomous weapons systems can be a source of fear, a key challenge might be the potential *imperfection* of such systems. As they are guided by technologies such as machine learning, the activities of LAWS might not be easy to predict, and desirable results might not be guaranteed. This also raises the question of whether and how ethical standards and international law could be incorporated into the algorithms behind the weapons systems.

The potential unpredictability of LAWS might also mean that they will not be widely used. There needs to be a certain level of trust and confidence in the technology before it could be employed for military purposes.

2. Proliferation and the arms race: Toward mutual destruction or deterrence?

Many fear that states that are developing LAWS will not be able to prevent their proliferation over time, which could result in a global arms race. There are also concerns about the use of such systems by domestic actors against their own populations, as well as by terrorist groups and non-state actors. In this regard, some raised the question to what extent the development of such technologies by private companies could be regulated.

The proliferation of LAWS could have important implications for international peace and security, although we can only speculate on how these consequences might develop. For example, a situation of mutual deterrence between nations possessing LAWS might develop, but there is also concern over possible mutual destruction.

3. Humanity in conflict: Should we outsource life and death decisions?

Many argue that machines are unable to replace humans in the qualitative judgements that form the basis for lethally targeting an individual. Making such decisions requires compassion and intuition, attributes we cannot expect robots to possess. While LAWS might be able to make quick and precise decisions, they will not be able to evaluate contexts.

Outsourcing life-and-death decisions to machines would not only risk making the wrong call, it would also make war more inhumane and could lower the threshold for the use of force.

However, there are some who claim that automated weapons systems actually offer potential humanitarian benefits and generate less collateral damage. Machines might be able to make decisions more rapidly and of higher quality, which could in turn contribute to the protection of civilians and the proportionality of an attack. In addition, some point out that human beings are not always ethical themselves.

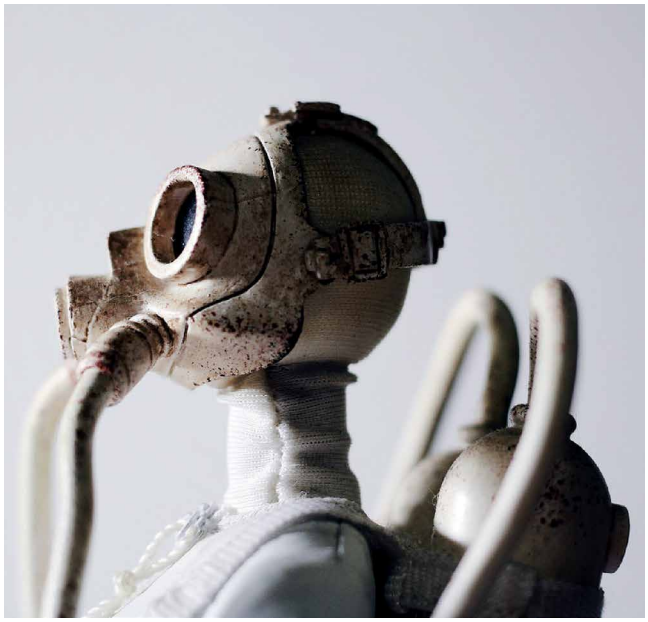
4. Responsibility: How can we hold a robot accountable?

One of the key concerns relates to accountability. If an autonomous weapon carries out a lethal attack, who is responsible? As LAWS encompass many nodes in a military chain of responsibility, it might be difficult to pinpoint who is accountable, and there are fears that unclear accountability could lead to impunity. Yet laws are applied to humans, and legal responsibility rests with those who plan, decide on, and carry out attacks. This responsibility and accountability cannot be transferred to a machine. In this context, some states also cautioned against providing autonomous systems with a legal personality.

5. Dual use: What if the force for evil is simultaneously a force for good?

The future application of AI and robotics in many civilian and economic facets of society, generated to benefit humankind, has led some negotiators to urge for caution on additional legislation, or a ban on LAWS. Yet, the dual-use nature of these technologies also means that autonomous weapons designed for civilian use might be turned into lethal weapons, adding to the complexity of the issue.

Read the full policy paper on the outcomes of the GGE on LAWS meeting.



Credit: Siyan Ren on Unsplash

THE GIP AT THE 12th INTERNET GOVERNANCE FORUM

The Geneva Internet Platform will be actively engaged at the 12th Internet Governance Forum, in Geneva and online. Join us for the following activities, and stay tuned for just-in-time session reports and *IGF Daily* summaries.

1 JUST-IN-TIME REPORTING

The *GIP Digital Watch* observatory will provide just-in-time session reports from the IGF, and *IGF Daily* newsletters, which will be available on a dedicated webpage, at *dig.watch/igf2017*. A final report, published after the IGF meeting, will summarise the main themes. These will complement the dynamic updates offered through the observatory.

2 ART@IGF

This project will connect digital policy with art in an interactive and interdisciplinary exhibition of digital issues. The exhibition will use a subway map as a journey metaphor to explore different Internet governance issues (infrastructure, security, human rights, etc.), each depicted as a subway line in a different colour on the exhibition floor. As participants follow the different lines, they arrive at subway stations where digital artists display their perceptions of the core digital policy issues of the day.

3 WORKSHOPS

The GIP is co-organising the following workshops at the IGF:

Data governance and policy: Developing a curriculum (WS186)
Monday, 18th December, 09:00–10:30, Room XI - A

Data is at the core of modern society, from our digital footprint via e-mail and social media, through to big data analytics. Although data governance and policy require new skills and techniques, the demand for data policy experts is not being met by supply. This workshop will discuss a curriculum that should be used for capacity development, training, and academic activities to improve policy-making.

A Digital Geneva Convention to protect cyberspace (WS34)
Tuesday, 19th December, 10:40–12:10, Room XXI - E

As effective cybersecurity is critical to international peace and economic stability, the creation of a Digital Geneva Convention could play a central role in safeguarding citizens, infrastructure, and private companies around the world from state-led or state-sanctioned cyberattacks in times of peace. This workshop will bring together cybersecurity and technology policy experts from different stakeholder groups to raise awareness of the crucial issues of cybersecurity norms, the gap in international efforts, and reality, and to discuss a potential way forward.

In addition, the GIP and Diplo team will be involved in a number of other sessions, as speakers, *in situ* and online moderators, and rapporteurs.

4 VISIT US AT OUR BOOTH

The GIP and Diplo will have a dedicated booth at the IGF Village. Visit us throughout the week, to get your copies of the *IGF Dailies*, and other Internet-governance-related publications (including the latest issue of the *Geneva Digital Watch* newsletter, the *Introduction to Internet Governance book*, and the IG Acronyms booklet).

IGF GENEVA 2017 18-21 DECEMBER

SHAPE YOUR DIGITAL FUTURE!

ART@IGF