INTRODUCTION

In last year, there have been major terrorist incidents that shocked the public opinion including attacks in Canada (October 2014), France (January 2015), Nigeria (January 2015), Denmark (February 2015), Tunisia (March and June 2015), Kenya (April 2015) and Turkey (August 2015). Governments in those countries reacted by introducing new laws or expanding existing ones explicitly designed to fight the threat of terrorism. Governments in several other countries, including United Kingdom, Spain, Italy and Austria also pushed for new anti-terrorist legislation. Measures designed to curb terrorism are also currently debated at the European Union level.

The goal of this brief is to provide background information about these legislative initiatives. It is designed to focus the discussion about the response of governments in the wake of terrorist attacks. It provides basic information about new laws proposed or introduced in several countries, as well as the public response to those changes. The brief is also supposed to help the authors to fill in gaps in this account with the help of participants of the roundtable discussion, which will take place on November 11, 2015 from 11.00 to 12.30 at the Internet Governance Forum in Joao Pessoa. Comments and conclusions from the discussion at the IGF will be integrated into the final version of the report.

OVERVIEW:

- This brief covers several countries, in alphabetical order, which recently experienced terrorist attacks and decided to push for new anti-terrorist legislation or initiatives: Canada, France, European Union, Kenya, Nigeria, Tunisia, Turkey and the United Kingdom.
- The goal of the brief was to focus on those measures, which apply specifically to the online sphere. However, some other relevant changes are mentioned to provide background such as increased border security, air travel data collection and intelligence sharing.
- New legal measures were introduced in several countries to increase government capacity to monitor online activity. In Kenya and the UK some measures are specifically targeted to monitor the youth that can be drawn to terrorism.
- Governments around the world make use of the latest technologies, often imported from other countries, in order to upgrade their surveillance capacity.
- Several countries, including Canada, Tunisia and the UK introduced new criminal offense targeting broadly defined terrorist speech and propaganda online.
- Many civil society representatives criticize those measures as violations of civil liberties and human rights, in particular right to privacy and freedom of expression.
Canada

Summary

- Canada adopted its first Anti-Terrorist Act in 2001 as a direct result of the September 11 attacks.
- Two terrorist attacks occurred in Canada in October 2014, which prompted the Conservative government led by Prime Minister Stephen Harper to introduce Bill C-51 in January 2015.
- Bill C-51 received royal assent on June 18, 2015: most provisions are now law in Canada and constitute the new Anti-Terrorism Act 2015.
- The new legislation changes several existing laws, increased intelligence services’ powers and allows sharing of personal data between 17 government agencies.
- In October 2015, the newly elected Prime Minister Justin Trudeau from the Liberal Party promised to make changes to Bill C-51.

New legislation:

- Former Prime Minister Harper stated about the terrorist attacks: “This will lead us to strengthen our resolve and redouble our efforts and those of our national security agencies to take all necessary steps to identify and counter threats and keep Canada safe here at home”.
- **Goals of Bill C-51**: to stop the promotion of terrorism, prevent terrorists from recruiting others and disrupt plots as well as preventing attacks on Canadian soil.
- **Information sharing**: Bill C-51 enacts the Security of Canada Information Sharing Act, which allows information sharing for national security purposes between all government departments and 17 specified agencies.
- **Air travel controls**: Secure Air Travel Act, provides a new legislative framework for identifying and responding to persons who may engage in an act that poses a threat to transportation security or who may travel by air for the purpose of committing a terrorism offence. It also authorizes the Minister of Public Safety and Emergency Preparedness to establish a list of such persons and to direct air carriers to take a specific action to prevent the commission of such acts.
- **Promoting terrorism becomes criminal offence**: The amendments to the Criminal Code include a new offense in Article 83.221 (1): Every person who, by communicating statements, knowingly advocates or promotes the commission of terrorism offences in general — other than an offence under this section — while knowing that any of those offences will be committed or being reckless as to whether any of those offences may be committed, as a result of such communication, is guilty of an indictable offence and is liable to imprisonment for a term of not more than five years.
- **Seizure of ‘terrorist propaganda’**: the Criminal Code now provides a judge with the power to order the seizure of terrorist propaganda or, if the propaganda is in electronic form, to order the deletion of the propaganda from a computer system if made available to the public through a Canadian Internet service provider.

Public reception:

- **Broad definition of terrorism and terrorist propaganda**: Civil society, lawyers and academics have criticized Bill C-51’s definition in the new article in Criminal Code for lack of clarity and specificity as a potential threat to freedom of speech. It could be used to violate the privacy of Canadians and could be used to target groups critical of government policy.
- **Excessive government powers**: Increased information sharing between government agencies has been criticized as excessive and lacking balance. The collection of data by the government and ensuing information sharing threatens the privacy of citizens. This could in turn lead to profiling and Big Data analytics on all Canadians.
- **Lack of oversight** is also a matter of concern, as 14 of the 17 agencies aimed by the Act are not subject to effective independent review.
European Union

Summary:
- Policies on the EU level are driven by the terrorist attacks in France and Denmark and pressure from national governments for increased access to personal data.
- The killings of 7-9 January 2015 in Paris have triggered new proposals. A majority of those proposals outlined in these responses predated the Paris shootings. Some had until that point proved contentious as regards their efficacy, legitimacy and lawfulness.

New laws:
- PNR: On 15 July, the European Parliament adopted a proposal for the long-term storage (5 years) of passengers on all flights entering and leaving the EU. The data will be used for profiling of innocent individuals as possible serious criminals.
- Prevention of radicalization: proposals emerged about how to develop counter narratives on social media. The removal of extremist content was also mentioned.

Public reception:
- Civil rights groups have criticized the proposed new measures like PNR retention, invoking Human rights concerns and questioning the effectiveness of the proposals for counterterrorism purposes.
- The EU’s approach to counter radicalization has caused criticism across the political spectrum as being inefficient, inconclusive and possibly damaging to community relations.

France

Summary:
- Attack on Charlie Hebdo offices on January 7 and kosher stor on January 9, 2015 were commited by gunmen linked to al-Qaeda and Islamic State.
- French Patriot Act: “Loi relative au renseignement” was adopted in June 2015. It is the second expansion of French surveillance powers passed since 2013, when the government broadened its powers to search Internet metadata.
- The new law overhauls the entire legal framework for France’s surveillance operations from the ground up for the first time since the 1990s.
- French Constitutional Court upheld the law on July 23, but three dispositions were rejected.

New legislation:
- The provisions of the law allow a wide range of new surveillance techniques meant for the Internet age, including the collection of “metadata” about online traffic and the use of software that can monitor every keystroke on a computer.
- Intelligence services can use these tools without approval of a judge, though the government must still seek permission from an independent body created to oversee surveillance activities.
- French officials say they need authorization to use new spy tools, such as fake cellular towers that collect phone information, to counter a growing domestic terror threat posed by groups such as Islamic State.
- Amid opposition to the law, President François Hollande submitted it to the Constitutional Council. The Council struck down
  - the provision that would allow emergency surveillance without the approval of the prime minister or another minister in the government. The Court declared the measure is “evidently a disproportionate violation of the right to respect for private life and the confidentiality of communication”.
  - the section dealing with surveillance of international communications that would have allowed the interception of communications “sent or received” abroad because it was too vaguely defined.
- Attackers not radicalized online: French Minister of the Interior Bernard Cazeneuve repeatedly cited a report, which indicates that 90% percent of those drifting into terrorism do it on the Internet. However, according to the investigations of the French intelligence services, police and gendarmerie, recent terrorists who committed recent attacks were not radicalized online. Many
experts agree that videos distributed through social media play a minimal role in the recruitment process for jihadists.

Public reception of the new laws:

- The **UN Human Rights Committee**, tasked with reviewing France’s compliance with its treaty obligations, criticized the law giving the French government “excessively large surveillance powers”.
- Terminology of the law is so vague that it permits any kind of surveillance, argue lawyers and rights groups and asked for the surveillance hacking and other surveillance tools to be removed.
- “Black boxes and algorithms will create permanent surveillance,” said Sen. Cécile Cukierman of the Communist party during a debate in June. French Internet service providers and hosting companies will have to install a new system in their infrastructure to filter all traffic. The equipment has been called “black boxes”—that would comb Internet traffic for signs of terrorist activity. Opponents say such algorithmic detection amounts to mass surveillance.
- The law gives new powers for intelligence services to bug suspects’ cars and homes to collect images, sound and data. Legislators and civil society actors argue that allowing intelligence services to obtain from telecommunications companies real-time access to Internet connection data of suspected terrorists authorizes mass surveillance and violates civil liberties.
- **Lack of independent oversight**: instead of getting a judge’s approval, the Prime Minister would only need to seek the views of a new body, the "National Committee of Intelligence Techniques Control", without any need to abide by them.

Kenya

Summary:

- Kenya suffered from **large-scale terror attacks**, most recently at the Westgate Shopping mall in 2013 and at Garissa University in April 2015. Terrorist group Al-Shabaab committed the attacks.
- The government constantly increases anti-terrorism measures, expanding and centralizing surveillance data in a command and control center.

New legislation:

- **Increased surveillance**: security agencies have stepped up surveillance on social media to fight terror, focusing on the youth. Officials say surveillance on Internet usage shows the young people, especially in universities, spend long hours on terror-related websites learning how they can join the groups.
- **New security bill**: After attacks in late 2014, the ruling Coalition moved to introduce the Security Laws (Amendment) Bill. Despite protests, the bill curtails constitutionally protected rights. It weakens the legal safeguards for interception of communications by police, increases the purposes for which surveillance may be undertaken, and provides for broad powers to intercept communications for the otherwise undefined "National Security Organs".
- **High Court decision**: Kenya's High Court threw out key aspects of the new anti-terrorism law after a legal challenge by the opposition. Eight clauses were annulled, including those, which curbed media freedom and capped the number of refugees and asylum-seekers to 150,000. The government is appealing against the decision, referring to growing threats posed by militant Islamists.
- **New surveillance technology**: a was tender awarded to Safaricom Ltd (Kenya’s largest telecommunications provider) covering surveillance capabilities such as video surveillance technology that allows for face recognition and a centralized database to perform analytics and cross-referencing on the images captured.

Public reception:

- **Controversy around purchase of surveillance technology**: the decision to single-source the tender and award it to the mobile provider Safaricom lead to a suspension of the project by the Kenyan National Assembly’s Committee on Administration and National Security. Reasons:
  - project cost, the choice of Safaricom as the supplier, its technical capacity, and its foreign ownership
  - the opaqueness of the procurement and possible violation of procurement law, corruption allegations, and the secrecy, speed and purported urgency of the procurement
Human rights concerns: privacy and discrimination
- Discrimination: even before the introduction of CCTVs, Kenyan police conducted raids targeting persons of either Somali heritage, Muslim faith or both. The unregulated use of CCTV cameras will only catalyse such profiling.
- Privacy: The proposed Data Protection Bill, 2013, does not recognise images or video recordings of an individual as personal data. The introduction of facial recognition technology in the absence of clear regulation means there is hardly any protection from the abuse of collected images.
- Freedom of speech and association: the facial recognition system allows the identification of any person by name. Photos taken on the street or from sources such as social media sites can also be used and stored in a database.
- Lack of oversight: there is no independent public oversight body to regulate how the information collected. The Independent Policing Oversight Authority has a limited mandate.

Nigeria

Summary:
- Nigeria has experienced widespread and growing incidences of kidnapping, blackmail, terrorist attacks and abduction. The radical terrorist group Boko Haram claims responsibility for many of the violent attacks, predominantly in the northern regions of the country.
- Nigeria does not yet have any existing data privacy laws or legal provision for interception of communication. The current security challenges in the country are being used as the reason to take major security decisions and make national commitments without the necessary constitutional approvals.
- Various top government officials have called for the regulation of social media, referring to the US doing the same.

Response by government:
- The legal framework for the prevention of terrorism in Nigeria is essentially embodied in two enactments: the Terrorism Prevention Act (TPA) 2011 and Terrorism (Prevention) (Amendment) Act 2013. It took Nigeria 10 years after the September 2011 terrorist attacks on the World Trade Centre to come up with a comprehensive anti-terrorism legislation.
- Data retention: Nigerian mobile service providers intercept all forms of communication. Telecommunication service providers are compelled to provide their customers’ records to security agencies. This is under the Bill of 2013.
- New Surveillance technology: The Nigerian government signed a 40 million contract with a company that provides surveillance technology. In April 2013, news emerged that the Nigerian government awarded a security tender to the Israeli company Elbit Systems for the procurement of surveillance technology. This technology enables the Nigerian government to intercept all internet activity, and to invade users’ privacy at will. There is no enabling legislation for such an action by the government.

Public perception of the changes:
- Opposition: loud protests by civil society organizations, press and individuals who fear a drift back to Nigeria’s dictatorial past. There was a feeble attempt by the House of Representatives to stop the contract. But the government went ahead to purchase the expensive Elbit surveillance equipment.
- Privacy concerns: Without the benefit of judicial protection through any laws on privacy and data collection, Nigerians remain vulnerable to infringements of privacy. The lack of any meaningful judicial framework and oversight for the deployment of surveillance technology has not stopped government authorities pushing ahead with increased surveillance.
Tunisia

Summary:
- In 2015, terror attacks in a museum in Tunis and at a beach resort in Sousse claimed the lives of 60 people, mainly tourists. The Islamic State claimed responsibility for both attacks.
- Shortly after the second attack, the president of Tunisia declared a state of emergency and a new anti-terrorism law was adopted that replaces the one that had been in place since 2003

New legislation:
- On July 4 President Beji Caid Essebsi declared a state of emergency; it was lifted on October 2nd, 2015.
- On July 25 Parliament adopted a new anti-terror law, which:
  - brings back capital punishment for certain offenses after a 25-year moratorium
  - grants security services powers to use special investigative techniques, such as surveillance, interception of communication, recording of phone conversations, and infiltration of suspected terrorist groups by policemen, provided they obtain advance judicial approval
  - makes public expression of support for terrorism an offense
  - suspects can be detained for 15 days without access to a lawyer and courts can close hearings to the public and allow witnesses to remain anonymous to the defendants.

Public reception of the change:
- The law was broadly supported by secular and Islamist parties, but strongly criticized by NGOs and civil society.
- Criticized regarding the return of capital punishment, overly broad definition of terrorism that could allow the repression of acts that are not of a terrorist nature as defined by international law.
- Potential abuses due to easier access to surveillance methods
- NGOs found that the law granted security forces broad and vague monitoring and surveillance powers

Turkey

Summary:
- Turkey has been witnessing increasing political polarization and terrorist attacks. The Turkish AKP government has been confronted with a number of wiretapping and eavesdropping cases that shed light on corruption scandals.
- Since beginning of 2014, the government has the right to block access to web pages within hours without a prior court order.
- Blocking of social media services and websites occurred in the run-up to the election, and in the aftermath of the Ankara bombings in October 2015, heating up debates about censorship.

New legislation:
- To exert more control over the Internet, the government has amended Turkey's Law No. 5651 on the Regulation of Internet Publications.
  - **Large scale censorship:** The law has since been used to temporarily ban popular platforms such as Blogger, Last.fm, Vimeo, Wordpress and YouTube. Currently, Turkey blocks based on both IP and URL addressees. As of May 2015, 80,000 websites were banned based on civil code related complaints and intellectual property rights violations.
  - **Websites supporting ISIS** and al-Qaeda derivatives, however, are not blocked in Turkey. Sites like takvahaber.net and mustaqim.net, which openly disseminate ISIS propaganda, function as a recruiting tool and call to violence operate freely in the country (Arango, 2015)
- Since March 2015 new amendments give authority for blocking decisions to ministers who can justify their decisions by invoking protection of national security, public order, public health, prevention of crime, and protection of life and property.
• Cases of social media & website blocking:
  o On 6 April, access to Twitter, Facebook and YouTube, along with 163 other websites and specific links to the stories published by Turkish newspapers, was blocked in Turkey, on the basis of a court ruling. By the evening of 6 April, the ban was lifted as the platforms had removed the content that the court deemed illegal.
  o On 25 July, the Turkish government ordered the blocking of 65 popular dissident and Kurdish websites and temporarily slowed down Twitter and Facebook access. This follows the government’s air attack against the Islamic State and Kurdish forces in Syria. A few days earlier, Twitter was blocked entirely for a few hours.
  o On 20 July, an Isis suicide bomber killed 31 members of a youth organization who were visiting the South Eastern town of Suruç. The Turkish government, reacted by attacking Isis in northern Syria. Following the attacks, the government changed its policy and blocked the pro-ISIS websites they were previously allowed.

Public reception:
  • The European Court of Human Rights has ruled that Law No. 5651 is against the European Convention on Human Rights.
  • Lack of transparency: the Turkish authorities do not provide details on the blocking of websites and the number of court orders issued.
  • Political opposition, human rights groups, and the disadvantaged groups criticize Turkey’s descent into a police or surveillance state.
  • Blockings of global platforms in Turkey result in strong backlashes from all over the world.

United Kingdom

Summary
  • The Counter-Terrorism and Security Act (CTSA), introduced in February 2015 is the latest attempt to impede radicalization of youth in the UK.
  • CTSA introduces powers allows the seizure and retention of the passport of a person suspected of involvement in terrorism-related activity abroad, and authorize the temporary exclusion of persons from the UK if believed to be involved in terrorism.
  • CTSA imposed a new duty on certain authorities, including universities, to have “due regard” to the need to prevent people from being drawn into terrorism.
  • The UK government applies a very broad definition of ‘terrorism’, including action taken to advance any ‘political, religious, racial or ideological’ cause designed to influence the government of any country or international organisation or to intimidate any member of the public anywhere in the world.
  • Anti-terror laws also include broad new speech offences, like the ‘encouragement of terrorism’ which includes making statements that glorify terrorist acts.

Responses by the government:

• Filtering content: Legal measures specifically designed for filtering and blocking content online have not been introduced with CTSA. The filtering program for network-level blocking by ISPs is voluntary and began at the end of 2013.
• Data Retention and Investigatory Powers Act (DRIPA) of 2014 is the new legislation to enable telecommunications data retention.
• New measures introduced by CTSA in 2015:
  o Terrorism prevention and investigation measures (TPIM): enhancing existing measures to monitor and control actions of specific individuals within the UK. If the government believes a person is involved in terrorism-related activities, it can impose restrictions on movement, financial activity or communication.
  o Data retention: enabling the attribution of internet protocol (IP) addresses to specific individuals, which was not part of UK’s data retention policy before.
  o Aviation, shipping and rail: new border security measures regarding transport, like screening of passenger data and keeping no-fly lists.
Preventive deradicalisation measures: a duty for a range of organisations (including universities) to pay attention if people are at risk to “be drawn into terrorism”. The provision makes the program for people at risk of radicalisation on a statutory basis, which used to be voluntary. One section puts a legal responsibility on universities to “exclude extremist speakers, including requiring advance notice of the content of events.”

Very recently, the UK government proposed a new draft legislation that allows authorities to check retrospectively people’s internet connection records (IP logs) without having to obtain a warrant.

Public reception:

- Civil society actors, and in particular many universities and education institutions raised major concerns both about the intent and the unintended consequences of the new duty to prevent radicalization. More than 520 university professors signed a letter sent to the Guardian, describing the Act as “unnecessary and ill-conceived.” The points of criticism included:
  - Chilling effect upon debate and academic freedom within universities
  - Creation of an atmosphere of mistrust between staff and students (contrary to academic values)
  - New administrative burden to staff and institutions
  - The new legal duty being vague and not achievable
  - A deterioration in the reputation of UK further and higher education.

Review: In June 2015, a key report reviewing the UK’s legal framework for surveillance was released:

- The thrust of the report is a call for wholesale reform of Britain’s surveillance legislation. Conclusion: “This state of affairs is undemocratic, unnecessary and – in the long run – intolerable.”
- Some of the recommendations: making judges, not ministers, in charge of authorising surveillance, and improving oversight and redress mechanisms.

Sources / further reading

Canada:
- [https://theintercept.com/2015/03/30/new-canadian-counter-terrorism-law-threatens-environmental-groups/](https://theintercept.com/2015/03/30/new-canadian-counter-terrorism-law-threatens-environmental-groups/)

United Kingdom:


PI report: [https://privacyinternational.org/?q=node/596](https://privacyinternational.org/?q=node/596)

Report on investigatory powers review: [https://terrorismlegislationreviewer.independent.gov.uk/](https://terrorismlegislationreviewer.independent.gov.uk/)

Campaign: [https://www.dontspyonus.org.uk/org](https://www.dontspyonus.org.uk/org)


France


Kenya:

- PI report: [https://www.privacyinternational.org/node/99](https://www.privacyinternational.org/node/99)
- GISwatch report: [http://giswatch.org/sites/default/files/is_surveillance_a_panacea_to_kenyas_security_threats.pdf](http://giswatch.org/sites/default/files/is_surveillance_a_panacea_to_kenyas_security_threats.pdf)

Nigeria:

- Criticism of current counter-terrorism approach: [http://www.huffingtonpost.com/salmaa-elshanshory/-new-counterterrorism-approach_b_5420544.html](http://www.huffingtonpost.com/salmaa-elshanshory/-new-counterterrorism-approach_b_5420544.html)

PI report: [https://www.privacyinternational.org/node/372](https://www.privacyinternational.org/node/372)


Turkey:

- Policy paper: [http://policyreview.info/articles/analysis/internet-censorship-turkey](http://policyreview.info/articles/analysis/internet-censorship-turkey)
- Website on censorship in Turkey: [http://engelliweb.com/](http://engelliweb.com/)

Tunisia:


EU:

- PNR: [https://edri.org/eu-parliament_to_vote_on_pnr/](https://edri.org/eu-parliament_to_vote_on_pnr/)