Dialogue on Cyber Policies between Brazil and the EU: prospecting threats and opportunities of the cyberspace

PREPARED AND PRESENTED BY:

Prof. Paulo Esteves-Veríssimo, Univ. Luxembourg
(Senior External Expert)

FOR:
Brazilian Federal Government, SEPIN/MCTI

UNDER:
Dialogue on Cyber Policies, Brazil-EU

Action Code: CYBER0001
1. Introduction
2. Workplan and Timeplan
3. Definition of Concepts
4. Framework
5. Status quo of cyberspace w.r.t. threats
6. Analysis of cybersecurity strategies and policies
7. Analysis of privacy and data protection strategies and policies
8. Analysis of the European Strategic Research Agenda on Cybersecurity
9. Academic Landscape
10. Technology Landscape
11. Analysis of the deployment and capability of cybersecurity organisations in Europe and some 3rd countries
12. Final analysis and recommendations
- **Objective:** further promote the existing dialogue between Brazil and EU in ICT and specifically, on *cyberspace policies, security and privacy*. This project comprises two specific instruments:
  - Expert contribution providing an overview of the European cyber policies, with an emphasis on security and privacy, and impact on technology.
  - Preparation of an international mission to foster exchange of information and experiences between public officials responsible for the formulation and implementation of cyber public policies.

- **Specific objectives and results expected are:**
  - *Share experiences* in ICT cyber policy and learn the EU best practices in these fields;
  - *Strengthen ties* with relevant European organisations dealing with cyber policies.
  - *Enhanced mutual understanding* on cyber policies, programmes and governance;
  - *Increased interaction* between the European and the Brazilian societies in Sci&Tech
Framework

- European Union
- EU vs. USA
- Brazil
Framework
European Union

- Digital Single Market Strategy for EU
- Cybersecurity Strategy of the European Union
- Cybersecurity Strategic Research Agenda – SRA
- NIS, Network and Information Security Directive
- General Data Protection Regulation (GDPR)
Progressive challenge of emerging digital powers, to the US and EU leadership

Perspectives on transatlantic cooperation, in cybersecurity and cybercrime, under some post-Snowden shadows or conflicts:
- EU calls for a ‘European strategic autonomy’
- US claims digital supremacy
- invalidat(ion of) the EU-US Safe Harbour Agreement

Building trust and confidence – both in the digital environment and with regard to state behaviour – is a fundamental pre-condition.
Linhas principais da estratégia em cibersegurança e ciberdefesa (2008-12):

- O sector cibernético é um dos pilares da Estratégia de Defesa Nacional.
- A defesa do sector cibernético é confiada ao Exército Brasileiro (EB).
- O fulcro da capacidade operacional desta última reside no Centro de Defesa Cibernética do Exército (Cdciber), apoiado no entanto pelas organizações governamentais já existentes (ex. CERT-BR).


- Documento da responsabilidade do GSI-PR
Status-quo resumido (na nossa interpretação):

Em teoria, alguma separação de facetas na organização da cibersegurança e da ciberdefesa: civil, administração pública, segurança da informação → GSI-PR, caráter mais militar ao Centro de Defesa Cibernética do Exército → CDciber.

Na prática o binômio cibersegurança-ciberdefesa centralizou-se na realidade no EB: tem desempenhado meritoriamente funções de protecção puramente civis; vários projectos mobilizadores de I&D em cibersegurança foram atribuídos ao CDciber e a vários outros institutos de investigação militares.

No entanto, existe, também na prática, intensa actividade e competência real de várias instituições, no domínio civil, da cibersegurança, como o CERT-BR e a rede associada.

Finalmente, a capacidade de investigação académica tem aumentado sem cessar nos últimos anos (criação de uma conf. nacional centrada em seg., projectos e presença internacional)

O nível de maturidade das infraestruturas e empresas Brasileiras é reconhecido como baixo, para as expectativas, quer por especialistas, quer pelo Governo. A capacidade de defesa cibernética do Brasil era estimada em 1 na listagem de um índice internacional de avaliação que vai de 1 a 6. Situação dos sistemas da administração pública, avaliada negativamente pelo TCU em 2010.

Sinais positivos: reconhecimento e avaliação do nível de maturidade e das capacidades inerentes; impacto das revelações de Snowden terá acelerado essa busca de maior maturidade, capacidade e resiliência dos sistemas.

Coalescence of factors leading to an increased risk:

- the world is becoming an immense, interconnected, interdependent infrastructure;
- there are huge amounts of correlatable data and cheap storage capacity;
- there is increased exposure by individuals and organisations: social, economic and legal pressure to be “on-line”;
- however, there is also a steadily increasing rate of software vulnerabilities.
This leads to a threat landscape diagnosis which should influence the strategy and policy-making of any nation:

- powerful adversary actors;
- availability of sophisticated exploit tools;
- targeted attacks and advanced persistent threats;
- data correlations previously impossible;
- elevated risk in all cyber components.
Analysis of cybersecurity strategies and policies

- Cybersecurity Strategy of the European Union
- Network and Information Security Directive
- Cybersecurity Strategy of some European Countries
- Cybersecurity Strategies of some non-EU Nations
Topic matters in cybersecurity

- Cybersecurity vs. cyberdefence
- Security vs. Privacy
- Surveillance
- Mandatory vs. voluntary enforcement
- Deliberate weakening of systems
There are three fundamental areas of interest insofar as a nation’s cyberspace protection is concerned:

1. General protection of the critical information and infrastructures against cyber threats.

2. Protection of the critical information and infrastructures against cyber or other threats, of magnitude and severity prefiguring acts of aggression or cyber warfare.

3. Protection of the critical military and classified information and infrastructures against cyber or other threats.
Topic matters in cybersecurity

Cybersecurity vs. cyberdefence

- **Cybersecurity**
  - covers mostly mediate and proactive concepts, adequate to times of peace (inclusive of civil society, prevention, early warning, training and awareness, certification and auditing, fighting cybercrime, etc.).

- **Cyberdefence**
  - covers mostly immediate and reactive concepts, adequate to times of disturbance/damage (drastic, cyber and/or kinetic defence and/or counterattack/offense actions in the face of aggressions, fighting cyberwar, etc.).
Topic matters in cybersecurity
Cybersecurity vs. cyberdefence

- **Cybersecurity + Cyberdefence**
  - *global and general defence of the nation’s critical information and infrastructure*, with the supervision of defence forces
  - Some operational and efficiency merits
  - However, has the *risk of diluting the desirable separation of facets between civilian and military, typical of rule of law democratic states.*
  - evidence in report about the potentially serious problems caused by confusion and ambiguity of these concepts and, ultimately, the prospects of militarization of cyberspace
Security and privacy often seen as contradicting or conflicting objectives. Securitary trends:

- ‘privacy’ concerns the individual and can thus be sacrificed to the collective good, supposedly represented by ‘security’ of the nation.

This status-quo gave way to laws allowing:

- *systematic, sometimes unwarranted, monitoring and mass surveillance by nation states*,
- *and permissive de-regulation sanctioning pervasive data collection by corporations*, of citizens and corporations, national and foreign.
‘Privacy’ is ‘security’ from the perspective of a person about the confidentiality of its information (data and meta-data).

- “person” may be not only an individual but a collective person, like an organisation or a sector thereof.

In cases of blanket data collection, we can no longer talk about ‘one individual’, but potentially, the inhabitants of a nation.

- mass surveillance implies affecting the collective rights of a huge set of individual and collective persons of a whole nation, under the argument of ‘individual’ persons.

Seen from this logical viewpoint, it is inevitable to put in perspective:

- (i) the magnitude of the value destruction occurring by the massive capture, analysis, archive, use and misuse of this information for a whole nation;
- (ii) with its potential gains for the nation’s security, still to be fully demonstrated, in light of recent terrorist attempts and other events.
Western (democratic) governments are increasing the amount, coverage and depth of surveillance of citizens and companies, not always only inside borders.

Two key aspects have politically sustained this trend:
- “only (harmless) meta-data are collected”
- “blanket data collection is necessary to ensure nation security”

In some cases, there is ample (voluntary or forced) cooperation of private companies with government agencies, in easing and amplifying harvesting this data.
Distinctions are made in EU regulation and doctrine between data and meta-data, and between mass unwarranted and indiscriminate interception, and targeted lawful interception of Internet and telephony data for the purpose of law enforcement and crime investigation.

- Targeted lawful interception constitutes a necessary and legitimate instrument of intelligence and law enforcement agencies...
- Mass surveillance is considered a threat to civil liberties such as the right to freedom of opinion and expression, ... essential human rights in democratic societies ...
- Meta-data is information about the time, origin, destination, location, etc. Meta-data does not contain the content of communications.
- The lawful interception of meta-data is targeted surveillance required by law enforcement authorities and is not considered as mass surveillance.
Mandatory or voluntary nature of cybersecurity enforcement:

- CERT community, relying on voluntary participation and cooperation between private and public entities,
- or more muscular, under the aegis of security agencies and subject to stringent reporting and information sharing requirements.

The opinions of EU nations are diverse:

- How much dichotomy between cybersecurity and cyberdefence
- varying definitions of the divide between what is civil and crime, and what is military and (cyber) war.
Such policies can be divided into three categories:

1. **escrow security systems**, overtly defined and regulated, where a “master key”, allows “opening” encrypted comm’s.

2. **systematic communications interception**, or wiretapping, overtly defined and regulated, where a “surveillance architecture”, systematically intercepts, analyses and records data e meta-data.

3. **systematic subversion of communications and computing systems security**, or “backdoor”, either overtly, as proposed by some law enforcement agencies, or covertly, as stealthily engineered by intelligence agencies, for systematic interception and interference.
World has been witnessing a race to techniques that allow the discretionary control of computing and communication systems by defeating their supposedly effective security defences.

These come from essentially nation-state actors, but probably to be followed as an example by other powerful actors, if nothing is done to attend to this “arms race”

This state of mind leads to careless attitudes even in the stricter case of targeted lawful interception
This is a problematic debate where decision makers are often times either ill-informed or have vested interests.

Even in the case of just technically enabling lawful targeted interception, any measures (like the iPhone or the WhatsApp cases) which imply global weakening, many have many more risks than gains.

In this high-tech world, any measures that seem socially and politically right (like targeted surveillance) must be seriously assessed for feasibility, magnitude of negative impacts.
Maybe the best testimony on the topic of law enforcement access vs. systems security comes from Vice Chairman of the Joint Chiefs of Staff Admiral James A. Winnefeld

“But I think we would all win if our networks are more secure. And I think I would rather live on the side of secure networks and a harder problem for Mike [NSA Director Mike Rogers] on the intelligence side than very vulnerable networks and an easy problem for Mike and part of that, it’s not only is the right thing to do, but part of that goes to the fact that we are more vulnerable than any other country in the world, on our dependence on cyber. I’m also very confident that Mike has some very clever people working for him, who might actually still be able to get some good work done.”
Analysis of privacy and data protection strategies and policies

- **General Data Protection Regulation**
  - will enable people to better control their personal data; will allow businesses to benefit from simpler rules and reinforced consumer trust.

- **Data Protection Directive**
  - for the police and criminal justice sector - will ensure that the data of victims, witnesses, and suspects of crimes, are duly protected in the context of a criminal investigation or a law enforcement action; facilitates cross-border cooperation of police or prosecutors to combat crime and terrorism more effectively across Europe
Topic matters in data protection

- Targeted vs. Mass Surveillance
- Safe Harbour vs. Privacy Shield
Study of EP challenges two main justifications:
- Only (harmless) meta-data are collected;
- Blanket data collection necessary to ensure nation security.

Findings:
- The analysis of meta-data, can reveal very detailed information about the person who has generated it, people’s habits and associations.
- Government agencies are massively intercepting meta-data directly or through service providers, and infiltrate systems and networks.
Topic matters in data protection
Targeted vs. Mass Surveillance

Conclusions:

- **meta-data is by no means harmless**, and in what concerns equating the privacy risks of surveillance, whatever the governments’ strategies in this area may be, it must be considered that “meta-data ARE data”.

- On the other hand, the alleged legitimacy and necessity of blanket data collection to ensure the security of a nation must be put in contrast with the potential damage effected on individual and collective persons.
Safe Harbour declared invalid in 2015 by ECJ

New regulation, *EU-US Privacy Shield* (2016), somewhat mends previous asymmetry in relationships between the US and EU, in disfavour of the EU:

- Strong obligations on companies handling Europeans' personal data and robust enforcement
- Clear safeguards and transparency obligations on U.S. government access
- Effective protection of EU citizens' rights with several redress possibilities
The document was organised in three areas of interest:

- AoI 1: Citizen Digital Rights and Capabilities
- AoI 2: Resilient Digital Civilisation
- AoI 3: Trustworthy (Hyperconnected) Infrastructures

Research challenges and expected benefits are equated for a few common technological/scientific research topics:

- Fostering assurance
- Focusing on data
- Enabling secure execution
- Preserving privacy
- Increasing trust
- Managing cyber risks
- Protecting ICT infrastructures
- Achieving user-centricity
This section discusses the status quo in learning, and point directions for evolution.

For example, an analysis of proposals for CBKs (Common Bodies of Knowledge) for Information Security and Critical Infrastructure Protection, main themes of cybersecurity and cyberdefence, is made.

A very thorough and complete grid of professional skills related to cybersecurity is also provided.
These sections discuss the status quo in technology, and point directions for evolution.

The document does an exhaustive analysis of the technologies concerned with cybersecurity, and complements it with a discussion focusing technologies onto business and activity segments.

Privacy-preserving technologies deserve special attention.

A study of the global cybersecurity market is also provided.
Analysis of the deployment of cybersecurity organisations in EU
Cybersecurity capabilities in EU

- ENISA - European Network and Information Security Agency
- CERTs - Computer Security and Incident Response Teams
- EC3 - European Cyber Crime Centre
- Eurojust – European Court of Justice
- EDA - European Defence Agency
- Contractual PPP on Cybersecurity
Three strategic priorities: cyberresilience, cybercrime and cyberdefence.

Cyberresilience: Department of Homeland Security (DHS) is the formal leader.
- The DHS is responsible for securing federal civilian government networks, protecting critical infrastructure and responding to cyberthreats.

Cybercrime: the US has not designated any lead investigative agency.
- Numerous federal law enforcement agencies combat cybercrime, e.g. FBI’s cyberdivision.

Cyberdefence: the Department of Defence (DoD) plays a leading role.
- It is readily apparent from the DoD’s multiple publications that the US has become more open about its capabilities and willing to name its adversaries. The DoD is also increasingly encompassing in its response to cyberthreats over time, investing in both defensive as well as offensive cybercapabilities.

The US CyberCommand, whose military leader is also Director of the NSA, coordinates the whole operation.
Final analysis and recommendations

General recommendation

- The project report provides an extensive overview of the European cyber policies, with an emphasis on security and privacy, and impact on technology.

- It is our general recommendation that this information is read with a critical eye, since solutions existing in other realities should not be copied *ipsis-verbis*.

- However, we are convinced that the time is ripe for Brazil to perform a dramatic evolution in this sector, and we see no reason for that not happening.
Although not part of the ToR for this study, and by no means wishing to force any ideas or trajectories, we would like to offer some specific recommendations for Brazil’s strategy in the area of cyberspace and cybersecurity.
Final analysis and recommendations
Specific recommendations

- **RECOMMENDATION 1:** Many of the aspects covered in the above analyses w.r.t. the EU might be taken in consideration by Brazil in their evolution, in the several facets presented.

- **RECOMMENDATION 2:** The compared analysis of cybersecurity strategies and policies in the report may be useful for a quick review of the Brazil’s recent strategy. The recommendations and implementation guide from ENISA [33, 34] also offer a checklist of the process.

- **RECOMMENDATION 3:** The experience in Italy, of a framework for incrementing the maturity and resilience of the public administration and corporate systems [24], might help overcome the recognized problems of the Brazil ICT tissue.
Final analysis and recommendations
Specific recommendations

- **RECOMMENDATION 4:** Concerning industrial development, for example analysed in the EOS study in [23], the very few aspects where, for example, the potential of the EU may be hampered, are due to the multi-state nature of the EU, and Brazil, being a federation, has the same advantage of the USA in that regard, which is a winning point.

- **RECOMMENDATION 5:** In the same study [23], Brazil might get insight about where they are, by elaborating their own data in the several competencies tables of the study, e.g. in the market size vs. growth graphics, and see where they fit. The same applies for the SWOT analysis.

- **RECOMMENDATION 6:** The European Strategic Research Agenda on Cybersecurity analysed in the report [14] is an impressive document which is expected to guide the EU strategy in the area for the next years. Brazil can possibly get inspiration and even compete with the US and US in the future, if they act now with agility.
RECOMMENDATION 7: Concerning maturity, readiness and resilience, the situational assessment of Brazil, both with regard to cybersecurity and cyber defence, might benefit from a compared analysis to situations of crisis, trying to assess how Brazil would behave. As an example, the simulation study of the projection of Brazil into real situations such as Estonia, 2007; Georgia, 2008; Israel strike on Syria, 2007; Stuxnet attack on ICS, 2010; stealing of classified and confidential information, several cases. Another example could be cyberattack and cyber war games, as performed e.g. by NATO.
Final analysis and recommendations

- **EPILOGUE:**

  To end with, it is important to understand that the cyberspace is highly asymmetric and dynamic, there is no reason why Brazil, even starting later, cannot come to perform superbly in this domain, as they have done successfully in others, such as avionics and aerospace for example.