EURODÉFENSE

EWG 17 BIS - CYBER FINAL REPORT 23.11.16

Mandate

"To make recommendations on points to be included in a European Code of Conduct on matters relating to the monitoring and surveillance of electronic communications, as recommended in the Report by EWG 17 agreed by Eurodefense Presidents following their meeting at Luxembourg".

Introduction: The EuroDefense WG on European Cybersecurity has sought to reflect developments in the domain of cyber surveillance, as it affects relationships between Member States of the EU. This effort has gained added importance following the recent series of terrorist attacks in Europe. The role of electronic information gathering in the pursuit of terrorists and other criminals needs to be balanced by the safeguarding of citizens' rights.

Citizens need the reassurance that their privacy will not be arbitrarily invaded; whilst law enforcement and security agencies need to pursue their investigations to protect the public. Criminals and terrorists do not respect frontiers; therefore, investigations should not be hampered by bureaucratic obstacles. Recent events have highlighted the need for good cross-border and inter-agency co-operation. Establishing an EU Code of Conduct for the monitoring and surveillance of electronic communications will achieve good co-operation and security, safeguard civil liberties, increased public confidence and assist in the communication with the public. In this area, national laws and constitutional guarantees and arrangements differ: a code of conduct, falling short of legally binding status, represents a more practical approach than a full legal alignment.

Recent Developments: Developments this year have included the following, the second of which is particularly relevant to the privacy issue addressed by this paper:

- February 2016-EU and NATO signed a technical arrangement to enable the NATO Computer Incident Response Capability (NCIRC) to co-operate with the EU Computer Emergency Response Team (CERT-EU). This has the effect of potentially creating technical measures that will enable the NATO 'Article 5' capability to co-operate with the EU's 'Solidarity Clause' in respect of Cybersecurity incidents.
- April 2016 - The EU promulgated the General Data Protection Regulation (GDPR) which will come into force in May 2018. The GDPR addresses the commercial use of citizens' data and seeks to put in place measures to safeguard individuals' privacy.
- July 2016 – The EU adopted on 6th July 2016 the Network Information Security Directive (NISD). This directive urges member states to increase protection of critical infrastructure and digital networks and encourages institutionalised information sharing between them. The cumulative effect of these measures provides a basis for the safe and efficient use of the internet. The benefit of a Code of Conduct is that it would avoid any legal lacunae which might arise through the drafting of these various instruments.

Best practice - Two national examples.

The UK Investigatory Powers Bill currently undergoing parliamentary scrutiny has highlighted some points:

- There should be a presumption of privacy.
- The threshold for accessing Internet Communications Records (ICRs) should be related to serious crime and to national security.
- There should be an independent review of bulk interception powers.
- Review of these powers should be in the hands of the judiciary – not the executive.
- There should be a criminal offence of the deliberate misuse of powers contained in the bill.
- The definitions of safeguards and standards must be consistent.

In August 2016 the UK's Independent Reviewer of Terrorism Legislation assessed that the Bulk Collection powers contained in the Investigatory Powers Bill were necessary and proportionate.

In Germany, a law on foreign country signal intelligence for the Federal German Intelligence Service has just passed the second chamber of the Bundestag. It covers broadly similar ground to the UK Investigatory Powers Bill. It provides that citizens and institutions of other EU countries have much the same rights of personal data protection as German citizens and interception of their communication requires similar judicial oversight.

Discussion:

A Code of Conduct does not have the full force of law; with the attendant sanctions that arise. Nor is it a Treaty obligation along the lines of NATO's 'Article 5'. However, its adoption signals that signatories recognise the value and purpose of the Code and will strive where necessary to adhere to its terms and conditions. It can also be adopted into national legislation or international treaty arrangements, once it has gained sufficient acceptance. Additionally, the rapid evolution of Information Technology means that a Code could and should be amended more swiftly to accommodate developments.

In addition to the Code, for the purpose of national security in cyber EU states should make a clear statement of commitment for support and cooperation along the following lines, for the purposes of deterrence:

"The Member States of the European Union agree that a cyber-attack against state owned or state controlled cyber infrastructure of one or more of them shall be considered as an attack against them all and consequently they agree that each of them will in that case assist the State or States attacked with all possible means to identify the attacker or attackers, trace the parts of the World Wide Web or cyber infrastructure being used and take the necessary steps to help counter the attack.

"The Member States of the European Union will in such case immediately consult together in order to determine what common retaliatory measures can and should be taken".

Proposed Code of Conduct:

The Code of Conduct should apply to all European Union member states in relation to surveillance of their own citizens and institutions as well as to those of the European Union itself and to its other member states, inside and outside their territory. Citizens of other European Union countries should have the same protection under the Code as citizens of the country conducting the surveillance. Non-European Union European countries should be invited to also adhere to this code of conduct.

The scope of the Code includes not only surveillance within national territory and airspace, but actions across national boundaries, from space, and from the territory of another nation (including embassies), and embraces the integrity of landlines and lines in international waters.

1. There is a distinction between ***monitoring*** and ***interception***. The former is surveillance of electronic communications to identify patterns and threats, without reading individual messages; the latter includes reading mail. The reading of individual communications should be subject to judicial oversight. Details of how this works are for the individual nation to decide, but the idea is that there should be a process of granting warrants which is independent of politics and based on rules that are publicly stated.
2. The criteria for intercepting mail are: defence, security and combating crime, protection of economic well-being. These are understood to exclude gaining political or economic intelligence or advantage.
3. As regards the obligations to each other of European states, the state from which the intercepted communication is transmitted should be consulted when time permits, or informed afterwards when time does not permit.
4. It would be impractical, in an age when neither criminals nor terrorists nor communications respect national borders, for individual states to have a veto on interception by other states of communications from within their borders. But there should be openness between states about their surveillance practices.
5. Member states should share information about the means by which surveillance of individuals and entities is carried out, and about the procedures they use to approach service providing companies and their procedures for approval of surveillance. This information sharing will have a confidence building effect.

6. Personal data collected for reasons deemed appropriate by this Code of Conduct should only be shared with third parties for the same reasons that they were gathered.

FINAL REPORT DATED 23/11/16