EURODÉFENSE

EuroDefense EWG 17 : European cybersecurity policy

Remit: *"To consider the principles that should underlie the practices of states in conducting surveillance of communications outside their sovereign territory, and if possible to recommend guidelines that European states should support"*

Executive Summary

1. The leaks by Edward Snowden in 2013 of details of the surveillance by US and allied intelligence agencies of private communications have prompted debate about the relationship between the right to security and the right to privacy, and the controls that should exist on official surveillance of private communications, in particular of communications generated in another state. This EuroDefense paper recommends action to be taken on these issues on the European level, and includes a proposal for enhanced collective defence against cyber threats.

2. The paper assumes that security will remain the responsibility of nation states and that therefore the imposition of legally binding common rules and procedures is not on the agenda. Moreover the relationship between security and privacy is legally complex and differs in detail from state to state. Nevertheless it is the conviction of EuroDefense that there is an important contribution to be made at the European level.

3. The paper argues that:

    - A Code of Conduct should be agreed by member states setting out good practice in relation to the criteria for on the one hand gathering information in bulk about communications (without reading individual communications), and on the other intercepting and reading them. The code should specify good practice in how approval is obtained for such monitoring or interception, and include guidelines on the constraints and procedures related to the monitoring or interception (of)by one state of communications generated in another.
    - The code should encourage states to share information about best practice, not only on the governance of surveillance but also on threats to security and how to deal with them.
    - Consideration should be given by the EU to establish an 'Article 5' type guarantee to all EU Member States in the event of a cyber-attack. The language to be linked to the existing 'solidarity clause', Article 222 of the Treaty of the Functioning of the EU.

    - The EU and NATO should ensure that the language of the relevant text of Article 5 of the Washington Treaty and Article 222 of the Lisbon Treaty is harmonised such that no hostile act (cyber or other) by an external agency, non-state actor or foreign power should avoid sanction.

Introduction

4. This EuroDefense Working Group proposes action that can be taken at the European level. It recognises that action on cyber-security is being taken by individual EU Member States and by transnational organisations, such as the UN, the EU and NATO (as well as private and corporate actors). It is hoped that this paper will contribute to the on-going conversation about those cyber-security measures which could be developed at the European level.

5. The remit for this WG [cited above] invites the WG to consider the principles that states should apply in conducting surveillance of communications *outside* their sovereign territory. This WG recognises that the nature of the internet (the World Wide Web) effectively renders national boundaries irrelevant to users, whether legitimate or otherwise. However, unlike cyber criminals and terrorists, law enforcement is, apart from international arrest warrants and organisations such as EUROPOL, largely limited by national boundaries, which therefore act as an impediment to effective legal measures.

6. 'Security' in cyber space cannot be achieved simply by the imposition of either national civil or criminal law. Whilst this WG recognises the impossibility of achieving a perfectly secure world in cyber-space it ought to be possible for like-minded allies to agree on measures of co-operation designed to keep their citizens safe, to protect their national security assets and to ensure their economic well-being. Enforcing international agreements or codes of conduct relies on co-operation and goodwill, and on peer pressure against transgressors. This paper will seek to address those measures which EU Member States should support in the conduct of surveillance of communications outside their sovereign territory.

7. The right to privacy (as set out in Article 8 of the ECHR) is a qualified right which can be interfered with on grounds of both national security and the prevention of crime, so there can be no justified expectation of absolute protection. However, citizens may feel that the agencies of the state are examining their communications data and infringing their right to privacy without reasonable cause. Member states may discover that the agencies of a neighbouring state are carrying out surveillance on communications within their sovereign territory without official sanction.

8. It should be possible to address these matters via a series of protocols that allow freedom of action for government agencies to pursue legitimate national security and crime prevention goals and which protect the rights of citizens. In particular it ought to be possible for an accepted protocol to be established which enables law enforcement and security agencies to pursue terrorists or criminals.

9. Preliminary discussion on this matter by EuroDefense members has coalesced around two key areas for further enquiry:

- A code of conduct
- A Treaty based Guarantee of mutual assistance.

10. These two proposals put the EU's weight behind the enforcement of cyber security. A Treaty based guarantee offers a clear signal to external powers that where they are detected, and can be attributed, cyber-attacks will be dealt with accordingly.

11. Balancing security and privacy will remain a constant endeavour. It is hoped that this paper will contribute to an awareness of the need for continued vigilance, whilst suggesting measures which can be adopted at the European level.

A code of conduct

Proposal

12. A code of conduct would need to provide an agreed definition of the following main areas:

The purpose of monitoring: where possible linked to criminal law or national security requirements.

- Authorisation: where appropriate by a competent judicial authority.
- Oversight: preferably by an independent national body; possibly by a sub-committee of the national legislature.

13. A code of conduct should also ensure that the following areas are addressed:

- That the surveillance undertaken is precisely targeted,
- That the level of surveillance resources deployed is proportionate.
- That there are arrangements for the timely authorisation of surveillance of persons within the national territory or abroad; and in the latter case, where practical authorization should be sought from the 'target' state.
- That Protocols for the requesting of data should be agreed to cover surveillance activities undertaken beyond national boundaries – within the EU and beyond the EU. This could include the mechanism by which governments or government agencies establish working procedures for authorization *in advance* (where practical) and *post-facto* where advance authorization is impractical.
- A code of conduct should be linked where practical to existing EU measures, or to the European Convention on Human Rights.

14. The attraction of a Code of Conduct in the context of cyber security is that it both requires voluntary agreement and applies peer pressure to signatories. The weakness of a rigid legal agreement is that it would be hard to agree and would therefore result in a levelling down of standards. It would also risk the potential for misunderstanding about the interpretation of language. The result could be a weak agreement. A Code of Conduct would need to fit alongside existing EU legislation, and not risk establishing lacunae which create uncertainty of interpretation.

15. The current situation consists of working agreements between law enforcement and security agencies. Any proposed Code of Conduct must support these efforts. The risk of a code of conduct is that the resultant language would represent a political point of view, not a legal definition. The problem would be one of definitions e g Monitoring vs Surveillance and levels of intrusive surveillance. One possible definition could be: Monitoring is the observation of patterns; Surveillance is listening to or reading communications.

16. In the EU context the Court of Justice of the European Union (CJEU) struck down large parts of the 2009 Data Retention Directive as being disproportionate in regard to the retention of 'meta data'. Existing legislation was judged to be insufficiently precise and open to abuse. EU Member States have undertaken stop-gap legislation to ensure the legality of their actions pending a resolution of this matter. This is a reflection of the difficulty of ensuring that legislation keeps up with technological advances. A key definition will be what constitutes communications data and the content of those communications. A new category of 'Communications Data Plus' might be required to enable the surveillance of data from a variety of platforms via a variety of media.

17. Taking account of the varying roles of the security and intelligence community among member states will also be a challenge in any code of conduct. For example, in the UK the legislation which established its national Sigint agency (GCHQ) on a legal footing specifically gave it a role in providing assistance in the prevention and detection of serious crime. This is not the case in all European states.

Best Practice – information sharing

18. Information sharing is a proven manner by which cyber-attacks can be detected and defeated. A wide range of industry groups now share information on cyber-attacks as they develop in real time (e.g. the financial services sector). NATO and the EU are co-operating on developing doctrines and practices. At a corporate level, however, there is an understandable reluctance to reveal weaknesses. Measures adopted by both industry and regulators are designed to establish minimum standards. Effective oversight by legislators and transparency by government agencies should be developed as a norm.

19. Senior former members of the UK security services have indicated that in their view clear distinctions on what is legal are preferable to blurred boundaries. Therefore, the Code of Conduct must be clear in its formulation, providing a clear sense of what activity is permissible. Public servants and agents of the state need to know which side of the law they are on; citizens need to know that their governments are not breaching the law. Law enforcement personnel need actionable evidence to secure prosecution; if it is obtained improperly it may well be inadmissible in a court.

20. The sharing of information about the nature of evolving threats as well as best practice in cyber security will be a helpful if not a necessary adjunct to a Code of Conduct. A Code of Best Practice would enable industry, government and law enforcement entities to maintain a permanent conversation, without prejudicing their respective points of view. Information sharing will also enable stake holders to 'send signals' to others that a particular development was either desirable or undesirable.

An 'Article 5' guarantee in relation to cyber security.

21. The communique issued after the NATO Summit in Wales in September 2014 states that '***Article 5*** (of the Treaty of Washington of 1949) ***can be invoked in case of a cyber-attack with effects comparable to those of a conventional armed attack.***' The intent of the NATO declaration is to send a message to Russia, particularly with the Ukraine situation in mind. Russia has used cyber-attacks on Estonia in 2007 and Georgia in 2008. ***The Alliance is currently examining how the link between collective conventional defence will be linked to cyber defence***. At present the Article 5 Guarantee of the Treaty of Washington is considered on a case by case basis. [See Appendix].

22. In the context of the EU, such a guarantee would need to be added to the current 'Solidarity Clause' article 222 of the TFEU. This clause is intended to address the consequences of a terrorist attack or a major disaster. The clause is invoked by the EU Member State directly affected. Should such a guarantee be adopted, the EU would need to establish a contingency planning mechanism to give effect to the obligation.

23. A primary consideration in this case is the matter of the attribution of a cyber-attack. The current level of digital forensics is estimated by industry sources to be good enough to trace an attack back to its place of origin, but not yet good enough to stand scrutiny in a court. The 'Mandiant' report on a cyber-attack on the New York Times in 2013 attributed responsibility to a specific unit of the Chinese People's Liberation Army. The Chinese government denied being responsible for this attack, but this episode illustrates how efforts in digital forensics may soon enable precise identification of the point of origin of a cyber-attack. International co-operation **will** be of vital importance to establish the attribution of these attacks.

European level action

24. The EU adopted a Cyber Security Strategy in 2013 which sought to ensure that the EU's core values extend to the cyber domain. The Strategy also sought to protect the rights of citizens and ensure that all had access to the digital world. In promoting a resilient internet, the EU Strategy sought to align its cyber defence policy and capabilities with the Common Security and Defence Policy. On the international level the EU has sought to ensure that its efforts uphold international efforts in this arena.

25. The EU is also working towards complementarity with NATO. NATO's approach to cyber security has evolved since work began in this domain at the 2002 Prague Summit. Following the 2007 cyber-attack on Estonia the Alliance promulgated its first cyber defence policy in 2008, which was revised in 2011. The 2014 NATO Summit in Wales sought to re-emphasize the cyber dimension of the Article 5 guarantee (see above). It has also invested in Information Assurance (IA) measures to ensure the integrity of its own communications system.

26. EU – NATO co-operation is important because it should ensure that there is a seamless web which links Europe's civil infrastructure with the defensive apparatus. It also provides a model for an 'open internet' which other international powers will be encouraged to emulate. Within this context the primacy of the rule of law should serve as a reassurance to those who feel that 'cyber-security' is synonymous with snooping by 'Big Brother'. It could also prevent the creeping militarisation of cyber-space.

27. The European Parliament (EP) regards it as its role to provide a check on the activity of the European Commission (EC), as well as safeguarding the rights of EU citizens. This applies as much to consumer law as it does to privacy. Ensuring good legislation also enables the efficient operation of the economy and the avoidance of monopolistic behaviour by large corporations. It is understandable that the EP should seek to be reassured that measures regarding surveillance of EU citizens are proportionate.

Discussion

Matters relevant to a Code of Conduct

28. The Jihadist attacks in Paris and Copenhagen together with the Belgian police raid in Verviers in January 2015 left a total of 17 people dead, plus scores wounded. The London Jihadist inspired killing in May 2013 claimed another life. These events demonstrate the nature of the threat facing open societies from 'self-starter' and 'lone wolf' terrorists. The UK government considers that the Woolwich attack might have been prevented if Communication Service Providers (CSPs) had shared information on their networks with government agencies. One of the attackers was in communication with a Jihadist with links to Al Qaeda in the Arabian Peninsula (AQAP) .

29. The need for security services to pursue Persons of Interest often involves surveillance of their communications. This communication often crosses jurisdictional boundaries. CSPs are required to provide material relating to internet traffic when requested by judicial authority. CSPs that are not based in the EU may consider that they are not subject to judicial warrants issued by EU Member States.

30. The surveillance practices of EU Member States must be designed to protect the fundamental rights of citizens whilst enabling the pursuit of criminals, many of whom operate across national borders. Technological change will continue to evolve rapidly as the market looks for competitive advantages. Criminals and terrorists will exploit these developments. Legal measures should be able to respond swiftly once lacunae are identified. Regulatory arbitrage whereby criminals or terrorists seek shelter within a permissive regime should be eliminated.

31. Data gathering and retention by both national agencies and CSPs should be proportionate. Efforts should be made to inform the public of the measures taken to protect them, and the limitations placed by judicial authorities on the activities of law enforcement and security agencies. This will achieve a higher level of trust, and serve to maintain transparency. Blurred lines of accountability often reflect bureaucratic inefficiencies, which could allow criminals to remain undetected and which risks losing public goodwill.

Matters relevant to an 'Article 5' guarantee

32. External threats exist to EU Member States from espionage activities of state sponsored entities that seek to probe for weaknesses in National Security structures via 'social media' [approaches]. Therefore, the cyber threat has both an internal and external dimension. Common to both is a need for good protection. This can best be done by information for public awareness about 'cyber hygiene'. It can also be achieved by the sharing of threat information. This must be managed so that no one country represents a weak link in the collective cyber defence.

Recommendations

- A Code of Conduct should be agreed by EU Member States, and candidates for EU accession, which addresses the procedures for surveillance of their citizens conducted by national state agencies.
- The Code of Conduct should address the means by which surveillance of individuals or entities is carried out across national boundaries within the EU and beyond the EU.
- A Code of Best Practice should be encouraged, to develop confidence among stake holders to exchange ideas about evolving security threats and best 'cyber hygiene' as well as exploring potential areas of mutual concern.
- The authorisation of surveillance should be by judicial authority.
- There should be better communication with the public about when surveillance is carried out and what legal restrictions limit this. The ultimate aim of this activity is to keep citizens safe and to protect both national security and economic well-being.
- Consideration should be given by the EU to establish an 'Article 5' type guarantee to all EU Member States in the event of a cyber-attack. The language to be linked to the existing 'solidarity clause' [Article 222 of the Treaty of the Functioning of the E U].
- The EU and NATO should ensure that the language of both the relevant text of Article 5 of the Washington Treaty and Article 222 of the Lisbon Treaty are harmonised such that no act by an external agency, non-state actor or foreign power should avoid sanction.
- This Working Group will, as the next stage of its work, develop specific proposals for points to be included in the Code of Conduct.

Appendix

Article 5 of the Washington Treaty

The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.

Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security

Article 8 of the European Convention on Human Rights

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Article 222 of the Lisbon Treaty [Solidarity Clause]

1. The Union and its Member States shall act jointly in a spirit of solidarity if a Member State is the object of a terrorist attack or the victim of a natural or man-made disaster. The Union shall mobilise all the instruments at its disposal, including the military resources made available by the Member States, to:

(a) - prevent the terrorist threat in the territory of the Member States;

- protect democratic institutions and the civilian population from any terrorist attack;

- assist a Member State in its territory, at the request of its political authorities, in the event of a terrorist attack;

(b) Assist a Member State in its territory, at the request of its political authorities, in the event of a natural or man-made disaster.

2. Should a Member State be the object of a terrorist attack or the victim of a natural or man-made disaster, the other Member States shall assist it at the request of its political authorities. To that end, the Member States shall coordinate between themselves in the Council.

3. The arrangements for the implementation by the Union of the solidarity clause shall be defined by a decision adopted by the Council acting on a joint proposal by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy. The Council shall act in accordance with Article 31(1) of the Treaty on European Union where this decision has defence implications. The European Parliament shall be informed.

For the purposes of this paragraph and without prejudice to Article 240, the Council shall be assisted by the Political and Security Committee with the support of the structures developed in the context of the common security and defence policy and by the Committee referred to in Article 71; the two committees shall, if necessary, submit joint opinions.

4. The European Council shall regularly assess the threats facing the Union in order to enable the Union and its Member States to take effective action.

REVISED 16 APR 2016