GROUP BRIEFING June 2012

Attack against information systems (Cybercrime)

Rapporteur + Political Group + Nat.	Monica Hohlmeier (EPP,DE)
Report Number and Committee	2010/0273 LIBE opinions by ITRE and SEDE
Procedure	COD
Green/EFA Drafts(woman)man	n/a
Shadows	Jan Albrecht (LIBE), Reinhardt Butikofer (SEDE), [name] (ITRE)
Staff	Wouter van Ballegooij (LIBE), Tobias Heider (SEDE), Laurence Vandewalle (ITRE)

Background

In recent years, the **number of attacks against information systems** (computers and networks) – or, in common words, the **illegal entering of or tampering with information systems** or **cybercrime** - has risen steadily in Europe. Moreover, large-scale attacks against the information systems of companies such as **banks, the public sector and even the military**, have been observed in the Member States and other countries. New concerns, such as the spread of malicious software creating **'botnets' - networks of infected computers ('zombies') that can be remotely controlled to stage large-scale, coordinated attacks** - have emerged.

These new developments are taken into account in the **Commission's proposal on the revision of** Council Framework Decision 2005/222/JHA on which a **General approach was reached in Council in June 2011** (Council Doc. DROIPEN 11566/11). A **draft first reading agreement was reached with Parliament's rapporteur Monica Hohlmeier (EPP) in June 2012**.

The fight against cybercrime is one of the pillars of the Union's **Internal Security Strategy**. It is also reflected in a number of other measures, such as the **revision of the mandate of ENISA** (European Network and Information Security Agency,. Its **external security dimension** is underlined by the high level **EU-US working group on cyber security** and cybercrime and the involvement of NATO, which has a centre of excellence in Tallinn, Estonia.

Content

The **text on which a draft first reading agreement was reached in Council, contains the following criminal offences** that are **already contained in the current legislation**:

- **illegal access** (article 3; the access to the whole or any part of a information system by infringing a security measure, when committed intentionally and without right, at least for cases which are not minor);
- **illegal system interference** (article 4; the serious hindering of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering suppressing or rendering inaccessible computer data, when committed intentionally and without right, at least for cases which are not minor);
- **illegal data interference** (article 5; the damaging, deletion, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system, when committed intentionally and without right, at least for cases which are not minor);

- and include the **following new elements:**
- **illegal interception** (article 6; interception by technical means, of non-public transmissions of computer data to, from or within an information system including electromagnetic emissions from an information system carrying such computer data, when committed intentionally and without right, at least for cases which are not minor)
- **tools used for committing offences** (article 7; the production, sale, procurement for use, import, distribution or otherwise making available of the following with the intent that it be used fro the purpose of committing any of the offence referred to in Articles 3 to 6, at least for cases which are not minor
    - (a) a **computer program**, designed or adapted primarily for the purpose of committing any of the offences referred to in Articles 3 to 6; or
    - (b) a **computer password, access code, or similar data** by which the whole or any part of an information system is capable of being accessed.)

Furthermore in accordance with article 9 the draft first reading agreement **raises the level of criminal penalties** to a maximum term of imprisonment of at least **two years** (articles 3 to 7), **three years for illegal system or data interference** (article 4, 5) **by means of a botnet** (article 7) or **five years when committed by a criminal organization, causing serious damage or committed against critical infrastructure. Instigation, aiding, abetting and attempt of those offences** will become penalized as well (article 8). **Identity theft should be considered as an aggravating circumstance** (article 9(5)).

The text also contains provisions regarding **criminal liability of legal persons** (article 11-12) and **improvement of police cooperation** by strengthening the existing structure of 24/7 contact points, including an obligation to answer within 8 hours to urgent request (article 14). **States, public bodies, and international organisations are exempt** from provisions of the directive (Art. 2 (c)).

Key points for our group

Questions may be raised regarding the **effectiveness of the extension of criminal definitions** and **raising of criminal penalties** in the fight against cybercrime. We do not expect this to have a deterrent effect on the perpetrators. More is expected from **preventive measures such as better IT security and maintenance, including setting strong incentives for this.**

The real problem is **weak IT security and systems resilience**, based on sloppy programming, on lack of redundancy due to cost cuts, and on a lack of incentives for systems manufacturers to change this, combined with **"as is" provisions in standard software licenses**. Discussions in LIBE have produced a wide consensus that it therefore is **not enough to focus on criminal law measures, and that the effect of those is negligible**.

The **discussion on attacks against information systems should also be broadened** in terms of **liability of the state and software producers** for not adequately protecting themselves against cyber attacks (**duty of care principle, extenuating/alleviating circumstances**) We also need to **distinguish between situations where hacking occurs with criminal intent and where it exposes serious security problems** ("**white hat hacking**").

Compared to Framework Decision 2005/222, the use of botnets and identity theft are now additional aggravating circumstances (FD2005/222: only organised crime). The distribution of hacker software is now criminalised EU-wide for the first time, as well as illegal interception of data communication. Penalties are now raised from "effective, proportional and dissuasive" to maximum penalties of at least two 2 for normal cases (including distributing hacker software), 3 years when using botnets, and 5 years when committed in the context of organised crime, causing

serious damage, or committed against a critical infrastructure.

We did however achieve a number of safeguards by :

- including the option of excluding minor cases
- adding intent as a condition for criminal liability
- adding the requirement that a security measure needs to have been infringed as a condition for any access to an IT system to be a crime
- managing to get hacker "devices" out
- clarifying that distribution of hacker software is only a crime if done with the intent that it be used for committing a crime; and
- clarifying that violation of terms of use or of employment rules when using an information system is not "unauthorised access" in a criminal sense

As regards protecting "white hat hackers" as integral part of the internet's immune system we managed to achieve a very weak recital (6a bis) compared even to the initial LIBE orientation vote. It is made clear that reporting of threats, risks, and vulnerabilities is crucial and needs incentives. The crucial last sentence, however, is not clear enough and far away from creating obligations for member states: "Member States should endeavour to provide possibilities, so as to allow the legal detection and reporting of security gaps." **Therefore there is** no serious protection of white hat hackers

who find vulnerabilities in other peoples' information systems and report them. **We did however** start a debate at all and getting the whole EP united behind this.

As regards setting incentives for vendors and operators to increase security we managed to achieve a recital (12b) that emphasises the importance of better security. The relevant sentence is "Member States are encouraged to provide for relevant measures incurring liabilities in the context of their national law in cases where a legal person has clearly not provided an appropriate level of protection against cyber attacks."

We can say that we started a debate on the issue but the text provides no serious incentives for better security such as mandatory liability for negligence on the operator or vendor side.

This is one of the files frozen in retaliation for the Council position on Schengen. **We managed to get a number of important safeguards in, and the fundamental debate on better IT security is opened. However the directive is in many ways worse than the old framework decision. Higher penalties and the criminalisation of more practices and even tools not only mainly symbolic, but even risks criminalising well-intended "white hat hackers" and curious teenagers**. The problem was Council and a too weak negotiation strategy of the rapporteur at the very end**. The option of going into second reading was never seriously discussed**. The LIBE WG therefore decided to vote against the draft first reading agreement.

Strategy for Plenary

Vote in Committee

Vote of our group	
Vote of the others groups / Majority	

Strategy for the Plenary Session

Amendments to be tabled by our group	
Proposal: vote Greens/EFA group	
Possible majority	

PLENARY RESULTS

Final vote: *in favour / against / abstentions*
- Good results **- Bad results** **- Coalitions/majority**
Key (media) message
Useful RCVs