Proposal for the Dutch Computercrime Act III; *A critique*

Mr. F.W.J. van Geelkerken LL. M, M. Phil

The Swedish Law and Informatics Research Institute, Faculty of law, Stockholm University, 106 81 Stockholm, SWEDEN

Abstract*– *On May 2nd 2013 the Dutch government published a proposal for a new Computer Crime Act (CCAIII). This article contains an analysis of the proposed power for police to "hack" into a suspect's computer, highlighting three categories of problems related to this proposed power..

Key words – Computer crime, Proposal for law, Hacking, Powers of police, Cybercrime, High-tech crime, criminal law, Dutch law.

I. Introduction

This article will focus on the proposal for law by the Dutch government to amend the current Dutch substantive- and criminal procedural code with the aim of improving and strengthening the investigation and prosecution of computer crimes. One of the most striking proposed powers in that proposal, the power for police to – in plain words – "hack" into the computer of a suspect[1], will be reflected upon.

The article will have the following structure, section two will contain a short background sketch of current legislation, in section three the proposal itself will be elaborated on, and section four will contain an elaboration on the proposed article which would enable police to hack into the automated work of a suspect. In section five a number of (potential) problems and risks related to the Proposal will be highlighted and the sixth, and final, section will contain comments, questions, and general recommendations to the Minister[2] and a summarising conclusion.

II. Background

The Dutch government formulated a proposal for the first Computer Crime Act in 1989[3] which, after having been amended several times, was enacted in March 1993.[4] The considerable advances made in the field of both information-, communication- and computer technology[5] (hereafter ICT) in the preceding ten to fifteen years, however, not only made it possible for organisations to store and process more and larger amounts of personal data, it also increased the possibility for states to monitor c.q. carry out surveillance of its citizens on an unprecedented scale.[6] The monitoring and carrying out surveillance of citizens by police can, however, also be very beneficial for law enforcement, as it makes it possible to more easily identify and/or localise a suspect. It would make it, for instance, possible to quickly identify a suspect by analysing the network level messages[7] sent by his computer or by triangulating the location of his mobile phone.

This situation might give rise to the notion of an Orwellian society, in which 'Big Brother' is always watching[8], but the benefits of monitoring c.q. carrying out surveillance should not be overlooked. The risks and benefits of monitoring the behaviour of citizens should be carefully balanced, which is amongst others why the proposal for the Dutch Computer Crime Act II[9], which created and expanded a number of investigatory powers for Dutch police, was only enacted in 2006[10] after having been under deliberation for several years.[11]

On May 2nd 2013 the Dutch government published a proposal for law for Computer Crime Act III[12] accompanied by an 87(!) page Memorie van Toelichting[13] which signifies the government is aware of the need for a careful balancing of the risks and benefits of expanding the powers of police. Considering the results of the third Cyber Security Assessment Netherlands, [14] the Proposal – which amongst others strengthens the powers of police to combat computer crime – could not come at a better time.

III. The Proposal

The proposal consists of three parts, the first part focuses on substantive criminal code. Next to a redefining of art. 54a (exculpation for a communication intermediary), article 80sexies has been rewritten and it contains a number of proposed criminalisations for amongst others; the copying of data from a non-public automated work (art 138c); the "fencing" of data (art. 139f), and the non-compliance to the (proposed) decryption order of a public prosecutor (art. 184b).

Article 80sexies has been rewritten to read "an automated work is an apparatus which is intended to, through electronic means, process and store data *or* to transfer it."[15] The first proposed criminalisation– copying data from a (hacked) non-public automated work – is in essence an additional criminalisation next to the (already existing) crime of breaking into an automated work.

The second proposed criminalisation – the "fencing" of data – criminalises the ownership, sale, trafficking, or use of non-public data if the suspect knew or should have known the data were obtained through a crime. Next to that, an exemption provision has been added for those who make data public for the public good (so called "whistle-blowers").

The third proposed criminalisation – non-compliance to a decryption order – is rather straight forward in the sense that if a suspect does not comply with the order of a public prosecutor to supply decryption keys and/or decrypt specific encrypted files he or she can be sentenced to up to 3 years of jail, combined with a fine of up to €19.500.

The second part of the Proposal focuses on criminal procedural code. Next to some – similar to the first part – redefined- and reformulated articles and headings, three different new powers are proposed. First, the power for police to hack into the automated work of a suspect (art. 125ja), second, the power for a public prosecutor to order decryption c.q. disclosure of encryption keys of encrypted files (art. 125K section 4), and third, the power for a public prosecutor to issue a notice and take down order to a supplier of a communication service (art. 125p).

As stated earlier, in section three the proposed power to hack into a suspect's automated work will be elaborated on in detail.

As to the second power, article 125k section 4 article states that a public prosecutor can order the decryption c.q. disclosure of encryption keys of encrypted files. Such an order could seriously violate the principle of nemo tenetur – the right to not incriminate oneself – which is why this power is strictly clausulated. In the memorandum[16] the Minister argues that – because of the invasiveness of this power in light of article 6 ECHR – the situations in which such a decryption-order can be used is limited to two situations c.q. two kinds of suspects. The decryption order can only be given to either a suspect of a terrorist crime or a suspect who either makes a living of the sale, spreading, or production of child pornography or habitually possesses and/or spreads child pornography.

The third power – issuing a notice and take down order – in essence gives the public prosecutor the power to order a supplier of a communication service i.e. an ISP, website, or e.g. an FTP-host, to immediately make specific data inaccessible to stop a crime or prevent future crimes. The third part of the Proposal contains general comments regarding the status of the Proposal.

IV. The power to hack

In the memorandum the Minister gives three reasons for the need to hack into the automated work of a suspect;

1. The problem passive- and active encryption poses for law enforcement;
2. The use of wireless networks and;
3. The use of cloud-computing services.

According to the Minister the use of (free) encryption software like TrueCrypt, and passive encryption like that used by Twitter, Gmail, and Skype decreases the effectiveness of Internet-taps more and more. Even though through the use of Internet-taps police (still) obtain a lot of communication data, more and more often the data they obtain is encrypted. Meaning that without the decryption key these data are useless for law enforcement. An added problem with the use of passive encryption like that used by e.g. Skype is that even if Microsoft (the owner of Skype) would be willing to supply the decryption key, they cannot because they do not have it and cannot decrypt the messages sent with Skype. [17]

Next to the problem of encryption, the nowadays more widespread use of wireless networks makes it more difficult to obtain a complete picture of the on-line actions of a suspect with an Internet-tap. Mainly because not all traffic will be monitored, and the use of wireless networks frequently results in traffic being monitored of innocent third parties who happen to use the same IP-address from a WiFi hotspot.

The third reason, the use of cloud-computing services, refers to the fact that nowadays more and more criminals use so called bulletproof hosting to spread e.g. child pornography. Providers of such hosting are most often located in countries with which the Netherlands has no legal aid agreements, and the business model of these providers revolves around their unwillingness to cooperate with foreign authorities wanting to identify their clients.

As such the Minister proposes the following article to create a power for police to hack into a suspect's automated work;

In case of suspicion of crime as described in article 67 section 1 [of the Criminal procedural code, FvG]*, which considering its nature or in connection with other crimes committed by the suspect results in a severe infraction of the legal order, the public prosecutor may – if the urgency of the investigation demands – order an investigative officer to enter an automated work or data carrier which is connected to it with the aim of;* [18]

1. Determining the presence of data, or determining the identity or location of an automated work.

The minister proposes the (digital) equivalent of the existing power for police to enter a location to establish the presence of for instance contraband. In the memorandum the Minister mentions as examples hacking into a smart phone to ascertain the identity of a person, hacking into a computer of which only the TOR-address[19] is known, or hacking into a router to obtain the MAC address[20] and other identifying characteristics of a suspect's computer. All of which would take place to be able to more selectively and better make use of (other) existing powers.

2. The copying of data in the automated work or connected data carrier to aid truth finding.

In the memorandum the Minister clarifies that the objective of this section is not to obtain communication-data but rather stored data on a suspect's automated work. Examples of such data are; images of child pornography, the storage of passwords of closed on-line communities, or decryption keys. Whereby, to obtain these passwords or decryption keys, the installation of a keylogger may be ordered, to prevent a public prosecutor from having to order decryption c.q. disclosure of encryption keys of encrypted files later on.

3. Making data inaccessible

This aim is rather straight forward in the sense that encountered data pornography in an automated work can be made inaccessible to stop on ongoing crime or prevent future crimes. Examples could be an FTP–server containing hacking tools, malware, or child pornography. Next to that, this power can be used to combat botnets, as disassembly of a botnet requires access to the servers within that network to remove the malware on individual bots. The minister clarifies that the inaccessibility of data is a temporary measure, in his ruling the judge determines whether the data needs to remain inaccessible or not.

4. "Tapping" and recording communication, recording confidential communication.

This section sees to the installation of policeware (spyware used by police) to covertly tap or record communication. Based on the memorandum this will take place primarily through the use of keyloggers or by turning on a microphone to eavesdrop on a conversation.

However, each time the use of policeware is authorised a new version of policeware will be written.

As such, depending on the needs of the situation the policeware will be developed differently; to record sound; to make screenshots, record keystrokes, or for instance to search specific file folders of the suspect.

5. Systematic observation

In itself this aim might seem rather odd, as the existing power of systematic observation has little to nothing to do with computer crime or searching a computer, but is a purely off-line activity. Nevertheless the Minister has included this aim rightfully so, for if the GPS, microphone, and camera of a smart-phone are activated in a smart phone, this results in a situation where all of a suspect's movements are being monitored very similar to that of the off-line systematic observation.

Based on the memorandum this option is meant for situations in which (off-line) systematic observation has not yielded (enough) results or in situations where the apprehension of the suspect is warranted but his or her whereabouts are unknown.

V. Risks and problems related to the Proposal

This article is too short to comment on all aspects of the proposed power for police to hack into the automated work of a suspect, especially because the Minister dedicates 37 pages on it in the memorandum, but in general the Proposal looks very sound. The memorandum is well structured, and contains a large number of examples to clarify the legal text. Next to that a number of safeguards to protect fundamental rights such as the right to privacy appear to be in place, and many potential problems have been forestalled with an explanation in the memorandum. Nevertheless, there are a number of potential problems or risks which have been left unaddressed by the Minister. These problems can be categorised as being practical-, general legal-, or procedural problems. Each category will be addressed under a separate sub-heading.

Va. Practical problems and risks

The first category of problems consists of four problems or risks of a more practical nature. These problems are not critical to the adoption of the Proposal in its current form, but the Minister might need to address them for the Proposal to become prevailing law;

1. Police will most likely be making use of "design flaws" or security weaknesses in automated works, which means police would benefit if those flaws or weaknesses are not patched, which in itself undermines the government's objective of increasing cyber-security.
2. The so-called "function creep", once a power has been granted to police – even if it may only be used under very exceptional circumstances – over time its use becomes more common and the use of the power becomes more and more accepted. A recent example is the amount of Internet-taps placed in the Netherlands which increased by 500.6% in 2012.[21]
3. The detection by anti-virus software, logically the policeware should not be detected by anti-virus software to be effective in their investigations. A number of security firms have however – as far back as 2007 – stated that their policy is to detect all spyware including police spyware.[22]

The minister has not explicated in the Memorandum how he would tackle this problem, despite answering parliamentary questions[23] about it in November 2012 with the statement "*the relation between the use of Policeware and anti-virus software will, as part of the practical problems regarding their use, be included in the preparation of the Proposal"*.[24]

4. The Policeware can be hacked, meaning that it would be usable by criminals to access the automated work of the suspect. Or worse – if the Policeware is not detected by anti-virus software – the government's software could be exploited by criminals for their own activities. Or *even* worse if the Policeware is hacked it could be possible for criminals to access the computers police *themselves* use.[25]

Vb. General legal problems and risks

The second category of problems and risks consists of three, more or less general, legal problems. These problems – in comparison to the previous category – are of a more serious nature, and the Minister will have to address these before the Proposal can be considered to become prevailing law. The basis for these problems is the fact that on the outset it is not always known whether an automated work which is going to be accessed by police is physically located in the Netherlands. (And thus whether the Netherlands has – or can claim – jurisdiction over the crime).

1. If police are allowed to access automated works of suspects which are physically outside of the Netherlands, those suspects are most likely also out of the Netherlands' jurisdiction, and these actions would infringe upon the principle of sovereignty and the rights of the people living in those states.
2. Allowing Dutch police to access automated works outside of the Netherlands (and the Netherlands' jurisdiction), without (iron-clad) bi-lateral and/or multi-lateral agreements, would be akin to an open invitation to other countries to allow their police forces to also hack into automated works in the Netherlands.
3. If Dutch police are allowed to exercise powers outside of the Netherlands' jurisdiction, this will create a precedent for other states to do likewise. Those other states might however have less-democratic regimes and may not incorporate as many safeguards as the Netherlands if they incorporate safeguards at all.

Vc. General legal problems and risks

Next to the aforementioned two categories of problems a third kind of problems, which can loosely be called procedural or legal technical problems, exists. A number of these problems touch upon the core of the proposed power for police to hack in the Proposal in its current form. As such these problems must be addressed, possibly by a rewrite of the proposed article 125ja, before the proposed power can become prevailing law.

1. With the proposed power, the right to privacy of not only the suspect but also of innocent third parties will be severely limited.Currently – when using a telephone- / Internet tap, or when installing covert microphones or cameras – the right to privacy of (innocent) third parties is already invaded because of their communication with c.q. presence near a suspect. If the proposed power for police to hack were to be implemented this would only make this situation worse. For the European Convention on Human Rights (ECHR) dictates that all measures which limit fundamental rights – such as the right to privacy – have to be necessary and proportional. This is amongst others why the government implemented the Privacy Impact Assessment Rijksdienst this year.[26] Based on this regulation the government has to make a PIA[27] before proposing any policy-change which limits fundamental rights. Withal, in the case of the Proposal – and more specifically the proposed power for police to hack – the Minister did not have a PIA made (yet).[28]

2. As stated earlier the Proposal also contains a revision of article 80sexies to redefine the term automated work to also encompass routers.[29] The phrasing of the proposed text, an automated work is an apparatus which is intended to, through electronic means, process and store data or to transfer it, is however (very) problematic. The definition as proposed would not only encompass computers, servers, and routers – the objective of the redefinition – but all computer-like devices which are connected to a network. As such not only the intended devices would fall under the definition but also for instance smart-phones, PDAs, tablets, GPS-systems, digital set top boxes, digital photo cameras with WiFi capability, onboard computers in cars, hearing aids, and pacemakers (and in the future Google Glass).[30] The proposed definition is especially problematic because what is, and more importantly what is not, an "automated work" has been interpreted restrictively in case-law, and through this proposed change this definition gets broadened.

3. On July 22nd 2013 the Minister published another proposal for law[31] to create a security- and data breach notification obligation for suppliers of services which are critical in, and for, Dutch society. The obligation to notify the Minister – and consequently other suppliers of critical services, and the public at large – of a security- and data breach could have an adverse effect on law enforcement if this obligation would also apply to a "breach" caused by police performing a criminal investigation. On the other hand if this obligation would not apply, the objectives of the proposal of July 22nd – enabling the NCSC[32] to assess the risks of the ICT-breach and aiding the victimised supplier[33] – cannot be achieved.

4. As the Minister rightfully points out[34] the integrity of the data obtained with the "eavesdrop" software has to be above suspicion. Despite the fact that the "eavesdrop" software will contain a logging function[35] that can register all actions of – and with – the "eavesdrop" software during its deployment, the data-integrity can still be called into question. First and foremost because the logs can be altered, but also because the data collected might get comprised through the collection method itself.[36]

5. The authenticity (and integrity) of the data obtained with the aid of "eavesdrop" software can be called into question unless police can prove beyond any doubt that the data as entered into evidence was not planted, or altered by police. In the Memorandum the Minister refers to art. 152 Sv[37] to prove the auditability of the power, but this is not sufficient. A written affidavit by a police officer about the investigation, collection-, and storage method of digital data which later one (might be) used as evidence does however not in *any* way safeguard the authenticity and integrity of that data, it only describes the actions of the officer.

6. The Minister proposes to regulate the use-, auditability-, and further technical aspects of the software to be used by police through specific governmental decrees and orders in council once the police's power to hack has become prevailing law. As Bits Of Freedom also points out in their reaction to the Proposal,[38] this is not an acceptable form of regulation. Based on the Proposal in its current form the police's power to hack – both technically and legally – will in essence only be limited by the software they are allowed to use. As such "filling in the details" about the software in lower legislation – after police are granted this power – is unacceptable as this would effectively remove any form of parliamentary scrutiny.

VI. Feedback and conclusion

As explicated in the previous section, the Proposal brings with it some problems and risks. In this section first a number of questions for the Minister are formulated in relation to these problems, to conclude with general comments on the Proposal.

1. Will police be making use of Zero-day exploits? And if so, will they notify vendors of the software in question there is a security weakness?

2. How will the Minister tackle the problem of detection by virus scanners? The Minister – in his reply to questions in Parliament – only stated that *"the relation between the use of Policeware and anti-virus software will, as part of the practical problems regarding their use, be included in the preparation of the Proposal."*[39]

3. What will be done to prevent the Policeware from being hacked and used by criminals?

4. Will the proposal of July 22nd 2013, creating a notification obligation for security- and data breaches, be applicable in the case of breaches by police?

5. How will the Minister safeguard the integrity and guarantee the authenticity of the data obtained through the use of Policeware seeing that a written affidavit is not sufficient?

6. Does the Minister agree that creating this "hacking" power for Dutch police without any (bilateral) treaties might lead to reciprocal "hacking" by other (friendly) countries?

As stated earlier this article is too short to do justice to all aspects of the proposed power for police to hack into the automated work of a suspect. Compliments have to be given to the Minister, however, for providing a very well structured Memorandum which contains a large number

of examples to clarify the legal text preventing the need for additional questions. Nevertheless, the Proposal in its current form cannot be accepted (at least regarding the proposed power for police to hack).

The aforementioned more or less practical problems are not insurmountable and might be resolved with some (extensive) clarification by the Minister. Similarly the general legal problems and risks elaborated on in section Vb do not necessarily make it impossible for the Proposal to become prevailing law, but these problems are of a more serious nature and will require a lot more attention of the Minister to tackle.

However, as stated before the third category of problems – the procedural / legal technical problems, expounded upon in sub-section Vc – touch upon the core of the proposed power for police to hack in the Proposal in its current form. These problems are so grievous they will probably necessitate a rewrite of the proposed power for police (if not a rewrite of the whole Proposal).

I would therefore advise the Minister to retract this Proposal, do a PIA before writing a new proposal, rethink the formulation of article 80sexies, and to not propose to further regulate through specific governmental decrees and orders in council, but to accept parliamentary scrutiny.

References

[1] "Hacking" is a maligned term, see A. Chandler, 'The changing definition and image of hackers in popular discourse', in International journal of the sociology of law 24-2, 1996. Historically there is a difference between the terms hacking and cracking, sometimes called white hat- and black hat hacking, nevertheless to prevent unnecessary confusion, hereafter the term hacking will be used to refer to remotely accessing an automated work without the owner's permission or knowledge.

[2] The Minister of Security and Justice hereafter referred to as "the Minister".

[3] Kamerstukken II (Parliamentary history of the Dutch second Chamber), 1989/90, 21 551, number 2.

[4] Staatsblad (official journal of the Dutch government) 1993, 33.

[5] The "umbrella" term ICT will be used to refer to Information Technology, Information and Communication Technology, as well as Information and Computer Technology.

[6] C. Diaz, O. Tene, and S. Gürses, Hero or villain: The data controller in Privacy Law and Technologies, p. 1, <http://www.cosic.esat.kuleuven.be/publications/talk-249.pdf>.

[7] Network level messages determine how a given communication will be sent and received. These messages, amongst others, contain the originating and destination IP-address of a communication and the sender's MAC address.

[8] Actually it would be more correct to speak of a large number of 'Little Brothers' see F.W.J. van Geelkerken, Biometrie; Gebruik van biometrische kenmerken in het BiB, <http://www. rechten-forum.nl/files/Biometrie.pdf> (Dutch only).

[9] Kamerstukken II, 1998/99, 26 673, number 2. (Dutch only)

[10] Staatsblad 2006, 300. (Dutch only)

[11] A first draft proposal for law was sent for consultation in January 1998 but Computer Crime Act II was not implemented and enacted until 1 September 2006, eight (!) years after its inception.

[12] Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III) (Change of the substantive criminal code and the criminal procedural code in relation to the improvement and strengthening and prosecution of computer crime (computer crime III)) <http://www.internetconsultatie.nl/computercriminaliteit/document/726> (Dutch only), hereafter referred to as "the Proposal".

[13] Explanatory memorandum, <http://www.internetconsultatie.nl/computercriminaliteit/document/727> (Dutch only), hereafter referred to as "the Memorandum".

[14] <http://www.government.nl/news/2013/07/03/cyber-security-assessment-netherlands-it-vulnerability-as-high-as-ever.html>, Kamerstukken II, 2012/13, 26 643, nr. 285 (Dutch only). See also <http://www.government.nl/news/2013/07/03/cyber-security-assessment-netherlands-it-vulnerability-as-high-as-ever.html>.

[15] Emphasis added in translation.

[16] The Memorandum, p. 49.

[17] See T. Berson, Skype security evaluation, <http://download.skype.com/share/security/2005-031%20security%20evaluation.pdf> whether this is analysis is still valid can however be doubted, see D. Goodin, Think your Skype messages get end-to-end encryption? Think again <http://arstechnica. com/security/2013/05/think-your-skype-messages-get-end-to-end-encryption-think-again/>.

[18] All translations by the author.

[19] See F.W.J. van Geelkerken, Egregious use of TOR-servers, <rechtenforum.nl files Onion routing.pdf>, 2007.

[20] MAC stands for Media Access Control. A MAC address is a unique identifier assigned to network interfaces for communications on the physical net-work segment.

[21] Kamerstukken II, 2012/13, 30 517, nr. 26.

[22] D. McCullagh/cnet.com, Will security firms detect police spyware?, 17-07-2007<http://news.cnet. com/2100-7348_3-197020.html>.

[23] Aanhangsel Handelingen II (Appendix Parliamentary questions II), 2012/13, nr. 739/751 (Dutch only).

[24] Infra 23.

[25] See for instance Chaos Computer Club, Chaos Computer Club analyzes new German government spyware, 26-10-2011, <http://ccc.de/en/updates/2011/analysiert-aktueller-staatstrojaner>.

[26] Kamerstukken II, 2012/14, 26 643 nr. 282. Whereby it should be noted that the motion by Senator Franken et. al. was instructive, Kamerstukken I (Parliamentary

history of the Dutch first Chamber) 2010/11, 31051, nr. D. (Dutch only).

[27] "A privacy Impact Assessment (PIA) is an aid to map, in a structured and transparent way, the privacy risks related to the development of policy, and the legislation or ICT-systems associated with that policy. The PIA-model is specifically aimed at the Government and meant for application in all policy-areas and within all areas of law". Kamerstukken II, 2012/14, 26 643 nr. 282- attachment, p. 1.

[28] Strictly speaking a PIA was not necessary at the time as the Proposal was published in May and the obligation of a PIA did not go in effect until September 1st 2013. Kamerstukken II, 2012/14, 26 643 nr. 282.

[29] The Memorandum p. 69-70.

[30] See Bits of Freedom, Reactie op consultatie Wets-voorstel Computercriminaliteit III, p. 5. <http://www.internetconsultatie.nl/computercriminaliteit/reactie/25502/bestand>

[31] <http://internetconsultatie.nl/meldplicht_ict_inbreuken> (Dutch only)

[32] Nationaal Cyber Security Centrum. <https://www.ncsc.nl/english>

[33] Explanatory memorandum accompanying the Notification of breaches electronic information systems Act (prop.) <http://internetconsultatie.nl/meldplicht_ict_inbreuken/document/782>.

[34] The Memorandum p. 27.

[35] "A feature which technically records the functioning of the technical aid [the Policeware, FvG] during its use". The Memorandum p. 27.

[36] As also stated by the Minister on p. 28 of the Memorandum, "[i]t cannot be ruled out that during the investigation, through the use of the software changes in the automated work will occur."

[37] "The [police officer] makes a written affidavit of the criminal act they investigated or of their actions and experiences in the context of their investigation".

[38] Bits of Freedom, Reactie op consultatie Wetsvoorstel Computercriminaliteit III, p. 8.

[39] Infra 23