Paper ACSERP

NATO cyber defense strategy in the Quantum Technology Era

Alexandru Ion

2016

ALPHA INSTITUTE OF GEOPOLITICS AND INTELLIGENCE

ACSERP
ALPHA CYBER SECURITY RESEARCH PROJECT

The Alpha Institute of Geopolitics and Intelligence
Paper ACSERP - Alpha Cyber Security Research Project

Roma, June 2016

The Alpha Institute of Geopolitics and Intelligence

ACSERP
Alpha Cyber Security Research Project

NATO cyber defense strategy in the Quantum Technology Era

Alexandru Ion

2016

Contents

Abstract

My research encompasses a multi-disciplinary area of international relations and security studies concerning NATO's strategic defense concerning the upcoming threat of the new quantum processors. The paper focuses on important issues that would change the cyber space making us rethink the design of our cyber security. Developing new encryption types would play a major role in protecting our information when using all means of communications.

Keywords: quantum computers, cyber security, NATO, cryptology

Introductions

As today's technology is progressing faster and faster, we are facing each day more and more threats from the internet. We currently have a total population of 3.366.261.156 world-wide using the internet daily on multiple platforms (Internet World Stats 2016). Under these circumstances, protecting our privacy is the main goal of our government and international organizations such as NATO. Through international collaboration in the past few years hundreds of hacking groups and malicious websites were shut down, this however has made little difference compared with underground activity of the internet. With the evolution of computers it is getting more and more difficult every day to stop cyber-attacks.

The innovating quantum theory has the potential of processing information 100 million times faster than the old super-computers, which will change our perspective on today's world, by making our lives much easier (D-wave 2015). But with the revolutionary technology come a new danger in cyberspace, as encrypted information becomes much more vulnerable to the new decryption power of the quantum processor, as many cyber security experts suggest (Naughton 2015). Although this new technology is still under development and only a few companies have access to it, mostly because of its price, in a few years it will become as wide-spread around the world as todays personal computers (Akama 2015, pp. 1-2). There is no available software at the moment in order to test the real performance for the quantum technology, but NATO should make it a priority on developing security software that can resist the cyber-attacks of this new type of processors.

Outdated security software as we saw in the past years have made computers vulnerable to attacks: Rocra, Mini Duke, Turla are just a few cases in which national information servers had faced malware actions known as cyber-spying in the last years (Monografia SRI 2015, p. 328). Losing this kind of information to foreign countries would mean lost years of work on research and development of military and governmental data.

Analysis on today cyber threats

To have a better understanding on the danger we will face once quantum computers will be available world-wide, we have to understand today's problems concerning cyber defense strategies. If we were to analyze statistics on cyber-attacks from last month, January 2016, we will discover that in 60% are cyber-crime motives and 27% of the cases are hacktivism, while the remaining 13% are cyber-espionage and cyber war cases. The targets of those attacks are: leading with 22% are the industries, in second place governments with 17% and 10% of the cases are single individuals (Hackmaghedon 2016). And those are only the cases that have been reported. There are many more victims of cyber-attacks that are unaware of the attacks until months later.

Providing a cheap solution on cyber security data breaches means that more and more individuals will use them, because most of the governmental computers use outdated software because of budget constrain (Cidon 2016). Symantec Corporation released in April 2015 a report on e-crime comparing the crime rate online of 2013 to 2014. This general overview shows us that the yearly increase of internet threats is becoming a serious concern for security both for the public and private sector. More than 317 million new malware were created in 2014 and 312 breaches in server information, a 26% increase compared with 2013 having 252 million malware and 253 breaches (Internet Security Threat Report 20 2015, pp. 88-90). If we are to take into consideration the statistics, we can estimate that by 2020 we will have on the internet around 1 billion new malware types and 1000 approximate mage-breaches on public and private servers. This information however applies only for the current generation of computers on silicon based processors.

If each citizen has at his disposal one quantum computer it would also mean that we need to redesign the encryption of our private communication. One of the first problems with the upcoming power of processing information by the quantum technology will be that the efficiency of the Advanced Encryption Standard 128 or even the 256 bit key unreachable until today wouldn't be considered a secured encryption anymore (Arora 2012). NSA has confirmed that the threat faced by the quantum computers is real and it's an impending danger on the long-term (Simonite 2016). Conceiving a new encryption algorithm capable of withstanding multiple quantum attacks is vital for maintaining the secrecy on the internet.

No.	Quantum Processor	Encryption type
1	D-wave 1 (2^{128} possibilities per instance)	AES 128 (2^{128} possibilities)
2	D-Wave 2 (2^{512} possibilities per instance)	AES 192 (2^{192} possibilities)
3	D-Wave 2X (2^{1000} possibilities per instance)	AES 256 (2^{256} possibilities)

Comparing evolution of quantum processors with the actual encryption keys

Outlining methods of countering quantum cyber attacks

The current methods used to protect our data will be inefficient with the introduction of quantum computers and that would mean we have to redesign our ways of defense in cyber space, since no one is immune. Financing research projects with universities would be an important step in order to transform theoretical ideas into practical security methods resistant to the new quantum cyber-attacks.

One of the ways to counter quantum computers would be to introduce a new encryption cipher to protect our data. Based on the new generation of cyber encryption like "Quantum key distribution" and "Honey Encryption" (Simonite 2014) there are new possibilities in which we can design our cyber algorithms to make them impenetrable (Dillow 2013). Designing an encryption similar to the "quicksand" method in which it would react by providing additional protection when brute force is applied would be enough to discourage hackers. With each attempt failed, adding additional new protection to the key would, without doubt, make this algorithm more complicated than the conventional ones. There isn't an impossibility to hack security mechanisms that can last forever, although designing an impenetrable solution for the next 5 years would be a good start.

Developing a strong partnership between the corporate sector and public sector based on cooperation is one of the fundamental keys of the future. Bringing together several of the most renowned cyber security companies to discuss the priorities and implementing the changes in the defense systems are considered matters of urgency. As I already underlined in the last chapter, having a cheap solution regarding the cyber defense means that more and more individuals will use it. While doing so, it is important to aim at developing sectorial methods of security then focusing on general aspects.

Conclusions

There are many threats in today's world that NATO has to face, but none is more dangerous than fighting against an unknown enemy through cyber space and, in order to do so, it must always be prepared. For NATO the cyber-attacks in the last couple of years in the cases of Estonia, Georgia and Ukraine were important lessons in what means to have a great defensive capacity for unexpected cases. Exploring new possibilities, simulating and learning from those events can provide us with an extensive feedback.

With the lunch of the new quantum processor D-wave 2X in 2015, known also as the fastest computer in the world, companies and institutes, such as Google, NASA, Lockheed Martin, USRA and University of Southern California, have confirmed that they use the computer for internal purposes (D-wave 2015). The list will continue to

grow every year due to the innovating technology used, and those institutions and companies are likely to start developing appropriate software for it. NATO should be the first international organization to develop the proper encryption, before the first quantum attack is reported.

In my paper I have provided a few solutions that can be applied to counter the cyber-criminal activity from the internet. There are many other alternative to improve our cyber defense system in the Quantum era, having yearly conferences and publishing papers on the subject will certainly help the rise of new strategies. For the moment I hope that I had contributed with my ideas to help NATO find new ways to develop the defensive strategy in cyber space.

Alexandru Ion
PhD Student at the Faculty of Political Science, University of Bucharest, Romania
ion.alexandru@fspub.unibuc.ro

Bibliography:

AKAMA, Seiki, *Elements of Quantum Computing: History, Theories and Engineering Applications*, Springer, 2015

Joan DAEMEN, Vincent RIJMEN, *The Design of Rijndael: AES - The Advanced Encryption Standard*, Springer, Bruxelles, 2013

GENNARO, Rosario, Matthew ROBSHAW, *Advances in Cryptology -- CRYPTO 2015: 35th Annual Cryptology Conference 2015*, Springer, Santa Barbara, 2015

Internet Security Threat Report 20, Symantec Corporation, 2015

James M. Kaplan, Tucker Bailey, Derek O'Halloran, Alan Marcus, Chris Rezek, *Beyond Cybersecurity: Protecting Your Digital Business*, Wiley Publishers, Hoboken, 2015

Monografia SRI, Editura RAO, Bucuresti, 2015

TAKAGI, Tsuyoshi, *Post-Quantum Cryptography: 7th International Workshop, PQCrypto 2016*, Springer, Fukuoka, 2016

Websites:

Asaf Cidon, Info security Magazine, *Government Security and Data Breaches: Problems and Solutions*, 2016. Available from: <http://www.infosecurity-

magazine.com/opinions/government-security-data-breaches/>. [16 February 2016]

Clay Dillow, Fortune, 2013, *Unbreakable encryption comes to the U.S.* Available from: <http://fortune.com/2013/10/14/unbreakable-encryption-comes-to-the-u-s/>. [15 February 2016]

D-wave, 2015, *Customers*. Available from: <http://www.dwavesys.com/our-company/customers>. [15 February 2016]

D-wave, 2015, *Introduction to the D-Wave Quantum Hardware*. Available from: <http://www.dwavesys.com/tutorials/background-reading-series/introduction-d-wave-quantum-hardware>. [2 February 2016]

Hackmageddon, *Motives behind the attacks*, 2016, Available from: <http://www.hackmageddon.com/2016/02/16/january-2016-cyber-attacks-statistics/>. [16 February 2016]

Internet World Stats, 2016. Available from: <http://www.internetworldstats.com/stats.htm>. [1 February 2016]

John Naughton, The Guardian, 2015, *The quantum computing era is coming… fast*. Available from: <http://www.theguardian.com/commentisfree/2015/dec/13/the-quantum-computing-era-is-coming-qubits-processors-d-wave-google>. [2 February 2016]

Mohit Arora, EE Times, 2012, *How secure is AES against brute force attacks*?. Available from: <http://www.eetimes.com/document.asp?doc_id=1279619>. [14 February 2016]

Tom Simonite, MIT Technology review, 2016, *NSA Says It "Must Act Now" Against the Quantum Computing Threat*. Available from: <https://www.technologyreview.com/s/600715/nsa-says-it-must-act-now-against-the-quantum-computing-threat/>. [18 February 2016]

Tom Simonite, MIT Technology review, 2014, *"Honey Encryption" Will Bamboozle Attackers with Fake Secrets*. Available from: <https://www.technologyreview.com/s/523746/honey-encryption-will-bamboozle-attackers-with-fake-secrets/>. [15 February 2016]