SPCSJ

SCIENTIFIC AND PRACTICAL CYBER SECURITY JOURNAL

VOL2 No2
June 2018

ISSN 2587-4667

Scientific and Practical Cyber Security Journal (SPCSJ) 2(2):1-4
Scientific Cyber Security Association (SCSA), 2018 ISSN: 2587-4667

MODIFIED ONE TIME PAD

Maksim Iavich, Zura Kevanishvili
Caucasus University, European School

ABSTRACT

Theoretically, quantum computers will be able to solve quickly the problems that classical computers would solve for thousands of years. This technology can change our world. A typical user will not need a quantum computer for a long time, maybe never. But using quantum computer it is possible to break all existing crypto systems. American mathematician Peter Shore invented a quantum algorithm that can factorize a large number into two simple factors very quickly. Unfortunately, classical computers make it very slowly. Classical computers can do it by sorting out all the combinations, but it will take million years. Safety of modern cryptographic algorithms is based on this weakness of classical computers, for example RSA. RSA BSAFE encryption technology is used approximately by five hundred million users in the world. RSA BSAFE is a validated cryptography library offered by RSA scheme. As we can wee RSA is the mostly used crypto system and it can be considered one of the most common public key cryptosystems that is developing together with development of Internet. Breaking RSA is a global problem and it can lead to breaking almost all the products in the world

One Time Pad (OTP) cipher is an example of a system with absolute cryptographic stability, this is system with perfect secrecy. It is considered one of the simplest cryptosystems. The biggest problem of one-time pad cypher is that it has one-time key. If the key is used to encrypt more than one message, the cypher is not secure.

In the article is offered the new modified variation of OTP, that is safe against quantum computer attacks.

Introduction.

Quantum computer is a computing device that uses quantum superposition and quantum entanglement phenomena to transmit and process data. Although the appearance of transistors, classical computers and many other electronic devices is associated with the development of quantum mechanics and condensed matter physics, the information between the elements of such systems is transferred in the form of classical quantities of ordinary electric voltage.

A fully-fledged universal quantum computer is still a hypothetical device. The very possibility of fully-fledged universal quantum computer needs the serious development of quantum theory in the field of many particles and complex experiments.

Developments in this field are related to the latest discoveries and achievements of modern physics.

Theoretically, quantum computers will be able to solve quickly the problems that classical computers would solve for thousands of years. This technology can change our world. A typical user will not need a quantum computer for a long time, maybe never. But using quantum computer it is possible to break all existing crypto systems.

In the 90s of the last century, the American mathematician Peter Shore invented a quantum algorithm that can factorize a large number into two simple factors very quickly. Unfortunately, classical computers make it very slowly. Classical computers can do it by sorting out all the combinations, but it will take million years. Safety of modern cryptographic algorithms is based on this weakness of classical computers, for example RSA.

RSA crypto-system with the key of length four thousand bits is considered safe from classical computers attacks, but it is vulnerable against attack of quantum computers [1,2].

To date, almost all valuable information that is transmitted over the Internet, is encrypted using RSA. This includes banking transactions, secret negotiations, and even your correspondence in social networks. Decipher all this with the help of classical computers is almost impossible.

Many products on various platforms in different areas use RSA encryption.

Now cryptosystem RSA is used by almost every commercial product, the number of which increases very quickly. RSA system is also widely used in from Microsoft, Apple, Novell and Sun operating systems also use RSA. RSA algorithm is used also in hardware; it is used in network cards, smart cards and Ethernet. RSA is used in cryptographic hardware also.

RSA algorithm is a part of the protocols protected Internet communications, like S / MIME, SSL and S / WAN.

RSA BSAFE encryption technology is used approximately by five hundred million users in the world. RSA BSAFE is a validated cryptography library offered by RSA scheme. As we can wee RSA is the mostly used crypto system and it can be considered one of the most common public key cryptosystems that is developing together with development of Internet.

As we see breaking RSA is a global problem and it can lead to breaking almost all the products in the world [3].

2. OTP

Vernam Cipher is a symmetric encryption system invented in 1917 by AT & T employee Gilbert Vernam.

This cipher is a kind of cryptosystem of one-time pad crypto systems. It uses boolean function "Exclusive OR"(xor). The Vernam cipher is an example of a system with absolute cryptographic stability, this is system with perfect secrecy. It is considered one of the simplest cryptosystems [4,5].

To get the cypher in one-time pad, message is xored with they key.

c= m xor k

For decryption cypher is xored with the message

m= x xor k

The biggest problem of one-time pad cypher is that it has one-time key. If the key is used to encrypt more than one message, the cypher is not secure.

Here we show the example where 2 messages are encrypted with the same key:

c1= m1 xor k

c2 = m2 xor k

if we calculate c1 xor c2 we get following:

c1 xor c2 = m1 xor k xor m2 xor k

c1 xor c2 = m1 xor m2

As we see cyphers can leak information about messages, if the messages are encrypted with the same key.

One-time pad is secure against attacks of quantum computers, so the biggest problem is the key distribution.

3. Modified scheme

Encryption: each letter in the message is xored with the corresponding letter in the key, so m[i] is xored with k[i] and like that is got the i-th letter of cypher.

Where m is the message and k is the key.

Afterwards m[i] is xored with the corresponding letter in the key, but in the inversed order, let us define the received number as x. So we add x random numbers to after i-th symbol in the cypher.

Decryption: The first symbol of the cipher is xored version of the first letter of the text and the first letter of the key. Thus this symbol can be reversed by being xored with the first letter of the key back into a letter of the text. Next the same symbol is being xored with the last letter of the key. The received number is the amount of pseudo random numbers present after that letter before the next letter of the message. These numbers are erased and the same process is then repeated for each letter of the cipher text until no more letters are left to decrypt.

5. Conclusion

In the new crypto system, we do not have already one-time key problem, the system is secure against quantum computers attacks, but must be mentioned that the scheme does not have perfect secrecy.

Must be carried out the work on the reducing of cypher's size.

Acknowledgement. The work was conducted as a part of joint project of Shota Rustaveli National Science Foundation and Science & Technology Center in Ukraine [№ STCU-2016-08]

REFERENCES

1. Gagnidze A.G., Iavich M.P., Iashvili G.U., Analysis of Post Quantum Cryptography use in Practice, Bulletin of the Georgian National Academy of Sciences, vol. 11, no. 2, 2017, p.29-36
2. Avtandil Gagnidze & Maksim Iavich & Giorgi Iashvili, 2017. "Some Aspects Of Post-Quantum Cryptosystems," Eurasian Journal of Business and Management, Eurasian Publications, vol. 5(1), pages 16-20
3. Bernstein D.J. (2009) Introduction to post-quantum cryptography. In: Bernstein D.J., Buchmann J., Dahmen E. (eds) Post-Quantum Cryptography. Springer, Berlin, Heidelberg
4. Bennett, Charles H., et al. "Quantum Cryptography." Scientific American, vol. 267, no. 4, 1992, pp. 50–57. JSTOR, JSTOR, www.jstor.org/stable/24939253.
5. Gu, B., Zhang, C., Cheng, G. et al. Sci. China Phys. Mech. Astron. (2011) 54: 942. https://doi.org/10.1007/s11433-011-4265-5
6. Kocher P.C. (1996) Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In: Koblitz N. (eds) Advances in Cryptology — CRYPTO '96. CRYPTO 1996. Lecture Notes in Computer Science, vol 1109. Springer, Berlin, Heidelberg
7. Boneh D. (1998) The Decision Diffie-Hellman problem. In: Buhler J.P. (eds) Algorithmic Number Theory. ANTS 1998. Lecture Notes in Computer Science, vol 1423. Springer, Berlin, Heidelberg
8. Dominic Mayers, Quantum Key Distribution and String Oblivious Transfer in Noisy Channels, Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology, p.343-357, August 18-22, 1996

Scientific and Practical Cyber Security Journal (SPCSJ) 2(2):5-9
Scientific Cyber Security Association (SCSA), 2018 ISSN: 2587-4667

DECISION MAKING SUPPORT FOR FORMATION OF COMPLEX SECURITY INFORMATION PROGRAMS. THE DISTRIBUTION OF RESOURCES

Serhii Zybin
State University of Telecommunications, Kiev, Ukraine

ABSTRACT

This article, written for analysis of a support decision-making approach. This approach can be used for the formation of complex information security programs, taking into account the threats and risks. This approach is based on the introduction of models and risks in the hierarchy of objective tasks and the goal evaluation of the tasks. Under the threat, we understand a condition of the environment, impacts the efficiency of the task. Complex goal-oriented program is executed in this environment. Risk is defined as a result of a random event that is caused by the influence of external relative factors. The event is a situation arises that affects the execution program. Threat models and risks have been proposed. The risk model is a risk factor, which is a random process and has a special goal. The threat is simulated by a special program, which is entered in the hierarchy of goals.

The stages of decision support technology taking into account threats and risks are developed and presented. These stages are based on the method of goal-oriented dynamic estimation for the complex program to ensure information security. The problem of programs (tasks) relative effectiveness that set by a multitude of threats and risks is solved. The task of using counteraction means to threats and risks is solved.

This article is the continuation of the articles [1, 2] and is devoted to the distribution of resources.

KEYWORDS: security program, decision making, protection system, DSS, decision support system, evaluation, simulating, judgement.

Improving the quality and reducing the time of decision-making when managing complex technical and information systems is not possible at present without informational and analytical support. Means of intellectualization of decision-making processes are the most important and practically necessary in the field of information security and information technologies.

Development and maintenance of complex systems found problems that can be solved only on the basis of a comprehensive assessment and accounting of different nature factors heterogeneous connections, environmental conditions and other factors. So increasingly important in modern conditions is a question of quality and efficient decision-making.

Problem solving of the information security can be obtained with the use of decision support systems. Decision-making is a compulsory step in any purposeful activities. Thus in the conditions of limited resources of all kinds, and increase of activities is continuously increasing difficulty decisions that are made, and the requirements for their efficiency.

The complex program to ensure information security is a set of activities united by unity of global goals and shared resources [3, 4]. The main objectives of the complex program to ensure information security development is a selection of programs to be included in the complex program and the resource distribution between programs. This complex program to ensure information security usually can be scheduled for long intervals of time, so we need to evaluate the effectiveness of programs in a given time interval.

It is necessary to take into account the possibility of threats and risks during developing the complex program to ensure information security. Analyze their impact and on this basis provide for measures to counter them or eliminate them.

We need to solve the following problems in the formation of the complex program to ensure information security considering the threats and risks:

- we need to determine the quantitative characteristics influence of threats and risks to the effectiveness of the complex program to ensure information security;
- we need to identify quantitative rates of the performance program considering threats and risks;
- we need to divide resources between counter means of threats and risks, and programs with goal to increase information security.

Known methods for solving the first problem include the identification of risks. This is a qualitative analysis. Moreover, provide the probability estimation and the size of the possible damage. This is a quantitative analysis [5, 6]. However, the problem of estimation program effectiveness into account of risk cannot be solved and remains at the discretion of the expert. Moreover, the definition of damage in absolute terms is often impossible for the complex program to ensure information security. The [1] article is devoted by this issue.

The [2] article is devoted to complex program to ensure information security, taking into account the threats and risks. The method is a modification of a method for the goal-oriented dynamic estimation of programs and tasks on a time interval.

This article is the continuation of the articles [1, 2] and is devoted to the distribution of resources.

The goal consists in developing of the support decision-making approach for the formation of complex information security programs, taking into account the threats and risks. Moreover, we should work out mathematical threat models and risks, efficiency estimate approach, and approach for the distribution of resources.

The problem solving method of evaluating the relative effectiveness considering threats and risks kindly develop based on the methods to solve this problem without taking into account these factors. The most common methods today got a multicriteria evaluation of programs [7]. The area of their application delimited by two conditions that must be satisfied by a specific task.

The first condition is the existence of multiple criteria, each of which can estimate a separate alternative.

The second condition is the ability of decision maker to evaluate in some way each alternative on separate criterion.

The first condition in the majority cases for the formation of complex programs do not performs because there are significant differences in the nature of the programs included in complex program. The second condition is very problematic, since the selection of the optimal alternative or ranking of a large number of variants requires taking into account of estimates for a large number of related criteria. This situation occurs when making decisions for the formation complex programs.
Therefore, methods of decision support during the formation information security programs considering threats and risks can be developed by modification of the evaluation variants goal-oriented methods [3, 4, 7]. The relative effectiveness of the programs should be evaluated as a time function, given at the planning interval [5]. Therefore, the possibility of taking into account the time factor in the evaluation of programs is fundamental for decision-making support tasks.
The task of resource distribution is to determine the set of optimal resources, which maximize the degree of the goal achievement. An algorithm of resource distribution between threats and risks and programs aimed at increasing information security [8] is proposed. The task of resources distribution can be formulated as follows.
There is a set of information security tasks: $T = \{T_i\}, i = \overline{(1,m)}$.
For each task, there is the degree of execution function, depending on the value of the resource $f(R_i / R_i^*), i = \overline{(1,m)}$,

where R_i^* is required quantity of resources;

$\overline{R} = \{R_i\}$ is option set (quantity) of available resources.

The calculation of efficiency corresponds to the vector $\overline{R}$. $E(\overline{R}) = E(\overline{F})$, where $\overline{F}$ is vector of the goal achievement degree.

It is necessary to find a vector R_x in which $E(R_x) \to \max$, when $\sum_{i=1}^{m} R_i \le R_{\max}$ is limited, where $R_{\max}$ is the resource quantity of the task [9].
We use optimization methods to solve the problem of resource distribution under the analytic function $E(\overline{R})$. In this case, resource efficiency is $E(\overline{R}) = \sum_{i=1}^{m} E(R_i)$. It is necessary to find such a vector R_x in which $E(R_x) \to \max$, when $\sum_{i=1}^{m} R_i \le R_{\max}$ is limited. This task is an optimization problem with a linear target function, that is, the problem of linear programming. The universal method of solving linear programming tasks is a simplex method. It allows you to solve linear programming problems with any number of variables and with any set limits.
The process of applying the simplex method can be divided into three main stages:
1) The preparatory stage. The problem should be converted from the linear programming to the canonical type with the best constraints.
2) The computational stage. We need to construct sequential simplex tables.
3) The final stage. We need to write the optimal values of the variables and the optimal values of the target function.

In the absence of an algorithmic problem solution $E(\overline{R})$, the solution of the problem is unknown, but to solve the problem, you can use genetic algorithms. For this purpose, it is necessary to calculate the efficiency at each point of the function. The obtained results are characterized by probability and require significant time expenditures that can be attributed to disadvantages.

We formulate goals and setting the tasks for the development of an algorithm for the threshold function of the execution degree with a linear hierarchy of goals [10].

The following primary data is specified.

In order to provide an adequate description of the tasks of efficient resource distribution, it is advisable to take into account changes in the availability of resources and threats over time.

There is a set of tasks to ensure information security $T(t) = \{T_i(t)\}, i = (\overline{1,m})$.

For each task there is a function of the degree implementation, depending on the size of the resource $f(R_i(t) / R_i^*(t)), i = (\overline{1,m})$, where $R_i^*(t)$ is the required number of resources at the time, $\overline{R(t)} = \{R_i(t)\}$ is the variant of the plurality (quantity) of available resources.

The set of thresholds $S(t) = \{S_i(t)\}, i = (\overline{1,m})$ for the function *f* is set.

The efficiency of using resources equals $E(\overline{R(t)}) = \sum_{i=1}^{m} E(R_i(t))$.

We need to find a vector $R_x(t)$, at which $E(R_x(t)) \to \max$, when $\sum_{i=1}^{m} R_i(t) \le R_{\max} \quad \forall i : 1 \le i \le m$ is limited, an equation $f(R_i(t) / R_i^*(t)) \ge T_i$ must be executed, where $R_{\max}$ is the number of resources of the task.

We create the restrictions $\forall i : 1 \le i \le m \; \exists \; f(R_i(t) / R_i^*(t)) \ge S_i$ in the form $\forall i : 1 \le i \le m \; \exists \; R_i(t) \ge S_i^*(t)$.

It is necessary to find $R_x = \{R_i\}, i = (\overline{1,m})$, such at which $f(R_1(t) / R_1^*(t)) + f(R_2(t) / R_2^*(t)) + ... + f(R_m(t) / R_m^*(t)) \to \max$, when $\sum_{i=1}^{m} R_i(t) \le R_{\max} \quad \forall i : 1 \le i \le m$ is limited, the equation $R_i^*(t) \ge R_i(t) \ge S_i^*(t)$ must be satisfied.

Step 1.

We insert the set of resources ratings $W = \{W_i\}, i = (\overline{1,m})$.

Then, the problem will look like the following view $f(R_1(t) / R_1^*(t))W_1 + f(R_2(t) / R_2^*(t))W_2 + ... + f(R_m(t) / R_m^*(t))W_m \to \max$, with the limitation $\sum_{i=1}^{m} R_i(t) \le R_{\max} \quad \forall i : 1 \le i \le m$, and the equation $R_i^*(t) \ge R_i(t) \ge 0$ must be satisfied.

Step 2.

We get $\overline{R(t)} = \{R_x(t)\}$, at which $E(R_x(t)) \to \max$.

Step 3.

We check the execution condition $R_i^*(t) \geq R_i(t) \geq S_i^*(t) \quad \forall i : 1 \leq i \leq m$ for all $\overline{R(t)}$ items. If the condition $\exists k : R_k < S_k^*$ is fulfilled, then *k*-th task is eliminated from the set of tasks and go to the step 4. If such elements are not found, then go to the step 5.

Step 4.

We will get a set of tasks $T_N = T / T_3$, where T_3 is the set of tasks that were received in the third step and which do not satisfy the constraints. After that, the transition to step 1 occurs.

Step 5. The end of the algorithm.

We get a vector S_x, as a result of the algorithm.

When the hierarchy has feedback, then the form of the efficiency function is nonlinear.

Conclusions

The task of resource distribution is to determine the set of optimal resources, which maximize the degree of the goal achievement. An algorithm of resource distribution between threats and risks and programs aimed at increasing information security is proposed.

The algorithm of resource distribution is proposed, when the function of the project execution stage is a threshold function. In this case, the hierarchy of goals is linear.

REFERENCES

1. Zybin S. The one method to decision making support for formation of complex security information programs. // Сучасний захист інформації: наук.-техн. журн. / Держ. ун-т телекомунікацій. – Київ: Вид-во ДУТ, 2016, № 4, С. 73 – 79.
2. Zybin S. The efficiency estimate method for formation of complex security information programs. // Сучасний захист інформації: наук.-техн. журн. / Держ. ун-т телекомунікацій. – Київ: Вид-во ДУТ, 2017, № 2(30), С. 49 – 56.
3. Тоценко В.Г. Методы и системы поддержки принятия решений. Алгоритмический аспект. / Тоценко В.Г. – К: Наукова думка, 2002. – 382 с.
4. Орловский С.А. Проблемы принятия решений при нечёткой исходной информации. / Орловский В.Г. – М: Наука, 1981. – 208 с.
5. Згуровский М.З. Информационный подход к анализу и управлению проектными рисками. / Згуровский М.З., Коваленко Н.И., Кондрак К., Кондрак Э. // Проблемы управления и информатики. – № 4, 200, с. 148-156.
6. Грачёва М.В. Анализ проектных рисков. / Грачёва М.В. Учебное пособие для вузов. – М.: ЗАО "Финстатинформ", 1999, – 216 с.
7. R.L. Keeney and H. Raiffa. Decisions with multiple objectives: Preferences and value tradeoffs. J. Wiley, New York, 1976.
8. НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу".
9. Руа Б. Проблемы и методы принятия решений в задачах со многими целевыми функциями // Вопросы анализа и процедуры принятия решений. М.: Мир, 1976. – С. 20 – 58.
10. Saaty, T. L. (2008) "Decision making with the analytic hierarchy process", Int. J. Services. Sciences, Vol. 1, No. 1, pp.83–98.

Scientific and Practical Cyber Security Journal (SPCSJ) 2(2):10-12
Scientific Cyber Security Association (SCSA), 2018 ISSN: 2587-4667

E91 NETWORK

Giorgi Iashvili, Aleksandre Lomadze-Gabiani
Scientific Cyber Security Association, European school (AHS)

ABSTRACT

E91, great as it is, becomes increasingly impractical as the network that it is implemented on grows. This is because as E91 only connects one end to another, so if one is trying to create a network using it they would have to store photons of every other device on each of the devices that are connected to the network. This requirement will cause the size of the devices on the network to bloat and make expansion and upkeep of the network extremely prohibitive. This paper suggests one modification of E91 that will make it more practical to implement.

To understand the modification that is being suggested in this paper we need to first understand several concepts; This part of the paper is meant to give a brief introduction to them.

1.1 Quantum Superposition

Particles can be described as probabilistic wave functions, which gives the likelihood of finding a particle in any specific position. Quantum superposition is the state in which the final state of the system is not known, therefore as Schrodinger's thought experiment posits the system exists in all the states at once. If the system is then observed, though the wave function “collapses” leaving us with a definite final state. To visualize this phenomenon in figure 1 there is a short animation of a qubit that has its wave function collapse several times because of an observer. [2] [1] In the figure (?) represents the state of superposition (↓) and (↑) represent different spins that were observed.

1.2 Quantum Computer

Quantum computers are a new type of computers that are on the horizon which are significantly faster than their classical counterparts. , and as qubits in superposition are at all points between 0 and 1 quantum computers are able to operate at all values at once (which by extension increases our computational power.)

This leap in the computational power of computers will obsolete asymmetric key cryptosystems such as RSA. Then because of this, we are forced to use symmetric key cryptosystems (at least until someone comes up with asymmetric key cryptosystem that is quantum computer proof) which creates a new problem of distributing the keys to and from authorized parties without evesdroppers being able to steal them. (which is the large part of why we even need quantum key distribution in the first place.) [1]

1.3 Quantum Entanglement

To put it simply quantum entanglement is a phenomenon when pairs of quanta (also known as EPR pairs) behave as a single entity. For example, if we were to observe the spin of one we would at the same time destroy the wave function of another and be able to actually get information about it (spins of the pairs are inverse of each other).Though sadly entanglement cannot be used for teleportation purposes we are still able to send random information across. [1]

1.4 E91 Protocol

E91 works as such:

1. parties have separated pairs of photons between each other.
2. They measure photons with randomly with one of two orientations
3. Information is shared classically where parties determine whether pairs of photons are actually anti-correlated
4. Parties then share more information about the orientations that they have used to measure the photons
5. If the orientations match then that information can be used in the creation of the private key.

E91 protocol is great because utilizing entanglement allows us to send information that cannot be intercepted. This, if used in conjunction with unconditionally secure classical elements, will potentially make the network utilizing E91 unconditionally secure. [1]

2. Modification Proposed

Modification proposed is to introduce servers (essentially middle-man quantum computers) between the user base, which will make the burden of size shift on servers (which are already big, so that additional size will cause much less trouble than bloating of other smaller devices on the network) ,and addition of new devices to the network will be made much easier.

So the problem that we are faced with is how do we transport the key from computer A to computer B with the relay server S. This means that computer A and B do not have each other entangled photons but they have entangled photons of server S which allows them to send random information to and fro the server (using E91 protocol).

The addition of the server poses one big problem in this case. After computer A observes its photons to send key 1 (K1) to the server that needs to be relayed to computer B The server is unable to control what spins the photons take when observed thus it cannot directly send the key with E91. To fix this my version the protocol proceeds as following - server observes entangled photons of computer B which sends K2 to computer B. Now the server encrypts K1 with K2 (with a cryptosystem of choice) and send it to computer Because computer B already has the key 2 it is able to decipher the ciphertext that is sent to it, and it is left with K1 in hand which

successfully accomplished the goal of getting the key from 1 spot to another safely so that now the communication can commence safely!

3. Flaws in The Modification

3.1 Unable to Use OTP with the distributed key

There is a flaw in E91 network if OTP is used to encrypt both the key that needs to be distributed (c1) and the message that needs to be sent(c2). This flaw occurs because of the security flaw in OTP itself, which posits that if two messages that were encrypted using the same key were to be XORed over each other there would result in a data leakage. So in the iteration of E91 network that uses OTP if eve were to intercept both c1 and c2 she would be able to glean some information that was exchanged. This critical flaw, therefore, eliminates OTP as a viable cryptosystem to use for both c1 and c2 so there is a need for another cryptosystem to be added into the mix.

Conclusion

In conclusion addition of servers as the layers of keys between separate instances of E91 can help with certain problems that we would face if we were to only use direct connections through E91. There are a few setbacks such as the high cost of running such networks because of which most from being able to enjoy the perks of E91 network, and a need to use something other than OTP for encrypting some data. The future research could attempt to tackle these or try and test E91 network in practice to get data about how safe it would actually be when put into practice.

REFERENCES

1. “Quantum Key Distribution Protocols and Applications”, Sheila Cobournem, Technical Report RHUL-MA-2011-05 8th March2011, https://www.ma.rhul.ac.uk/static/techrep/2011/RHUL-MA-2011-05.pdf
2. S.Singh, “The Code Book: the Secret History of Codes and Code - breaking” ,Fourth Estate, London, 1999

Scientific and Practical Cyber Security Journal (SPCSJ) 2(2):13-17
Scientific Cyber Security Association (SCSA), 2018 ISSN: 2587-4667

MODERN APPROACHES TO THE SECURITY EVALUATION: A ROADMAP TO SECURE AND USABLE SYSTEMS

A. Fesenko, H. Papirna
Taras Shevchenko National University of Kyiv

ABSTRACT

There is a huge number of different methodologies for evaluating the security of the systems. However, even the most reasonable of them turn out to be incompetent due to the omission of the importance of keeping user convenience in mind. This disadvantage has been resulted in the spread of secure, but useless, from the point of the performance of user tasks, systems. The aim of the article is to process and systemize the existing researches on the development and evaluation of systems, that include the human factor and users' needs. In addition to this, working recommendations has been considered to help developers and auditors of secured systems.

KEYWORDS: security evaluation, Human Computer Interaction (HCI), Human Computer Interaction and Security (HCISec).

1. Formulation of the problem

In a modern information world, where the use of computer systems has become widespread: from state structures and critical objects to large and small businesses, the problem of evaluating the security of the information system is urgent.

This need is due not only to state and international standards for the protection of information resources and information, the protection requirement of which is established by law, but also financial factors for business that arise in case of loss of critical information, unauthorized access to resources, or failure of the system.

When evaluating the level of security of information systems, there are problems associated with the following factors:

- variety of existing regulatory documents, regulatory data processing procedures, composition and content of organizational and technical measures for the protection of informational resources of various levels of confidentiality;
- lack of quantitative criteria for evaluating the security of information systems in normative legal documents;
- complexity, multicomponent structure of the evaluated information system;
- conditions of uncertainty and insufficient knowledge about threats and the probability of their realization for an information system;
- constantly changing information security incident statistics, including cyber threats that occur when connecting to the Internet [1].

2. Statement of the main material

After analyzing current international regulations of technical information protection, it becomes clear that approaches to evaluating the security of systems need some improvement.

Although actual criteria allow to evaluate the security of the system, they do not consider another important factor. The Human Computer Interaction (HCI) and Human Computer Interaction and Security (HCISec) have long been developing in the world. The popularity of these areas is due to the eternal struggle between the simple use of the system and the provision of an adequate level of security. Therefore, the evaluation of the security of the system is no longer possible in isolation from the convenience and ease of use.

The gaps and conflicts between security and usability have been carefully studied by several researchers. In [2] the author proposed to evaluate the security of the system by following guidelines or by using frameworks.

A working guideline with criteria for evaluating usability of secured systems has been outlined in [3]. It focuses on providing a checklist for software developers of secured systems.

According to this publication, the first and the main point is opened and understandable security for all users. It is the responsibility of the developer / deployer to hide as many security mechanisms as possible from the user. For those security mechanisms that are exposed to the end user it is necessary to get security awareness.

The second key point emphasizes the reduction of prohibitions for a user. A usable security mechanism should not be used to restrict the user in what he is doing but protect the user. This allows end users to efficiently fulfill their tasks. Any security-motivated restriction of the user should be carefully evaluated regarding necessity for system security and adequateness.

The next requirement highlights the minimum interaction of the security mechanism with a user and its role to grasp the user's attention. In addition to this, an efficient security system should not require the user to remember a lot of data. For example, the user can use an existing account to login and does not have to remember another password.

The following item considers the assurance that the average user is capable to make an informed security decision on the appeared issue. If it is not clear if the user can decide on an issue, the decision should be avoided.

Also, the user should not have to configure security when he first starts the system. It should always come preconfigured such that it is reasonable secure and usable. Another important issue is that a secured system should not use fear to force users to obey security policies or get a wanted reaction. It must always support a positive attitude of the user towards itself. Finally, a secured system should take into account that users tend to make mistakes, so the system must provide an explained response to the user and route the one to the right solution.Apart from guidelines, different frameworks and models can also be found in literature, that assist in addressing the conflicts between usability and security and provide critical factors to be investigated for evaluation of security and usability. A suitable example of such a framework has

been presented in [4]. According to this approach, to assess the security of the system, it is necessary to build a security–usability model.

To assess usability, the following criteria has been applied:

Effectiveness is measured by whether users can perform a specific task or not.

Satisfaction – although an objective analysis of usability is generally acceptable, a subjective evaluation of users is key to the success of the system.

Accuracy – requirements to which are driven by needs of users in providing the necessary information.

Effectiveness – using the system only to achieve a certain goal is not enough. The goal must be achieved within a reasonable time and effort.

To assess security, the following factors has been used:

Attention – security issues should not distract users from their work, as this will definitely lead to errors in security mechanisms and nervousness of users.

Vigilance – the system should provide users with the opportunity to be active and encourage them to instantaneously report about suspicious incidents in the system.

Motivation – users of the system should take every risk, as directed personally to them, in order to fulfill the security requirements more quickly.

Conditioning – the trivial types of frequently repeated security requirements should be avoided, as they are addictive and the user may inadvertently click on the wrong action in a critical situation.

Social context – users who work on one project are often inclined to share security secrets (shared passwords, certificates, etc.). The task of assessing the security of a system should take into account such a social experience.

As a general rule, there are two factors that combine security and usability:

Memorability – a large amount of information for authentication (passwords, secret words, etc.) threatens both usability (time to change the password) and security (writing down the secret information on a sheet of paper, etc.).

Knowledge and skills - the speed of user's learning of a system must be evaluated, especially to the security-related operations.

For a successful evaluation, both security and usability elements must be measurable. Therefore, auditors, after understanding the criteria listed above, should develop appropriate qualitative or quantitative metrics for system evaluation.

3. Development of recommendations

On the basis of the processed publications, it is possible to define recommendations [5] for the designers of the secured systems as well as for the system security auditors.

The first lesson to be concerned is that, the usable security cannot be retrofitted. The security community is completely sure that security must be designed into systems from the ground up; it cannot be "bolted on" to an existing system at the last minute. The same is true for usability of security. For example, adding explanatory dialog boxes to a confusing system is not the solution. Such fundamental design principles must be considered at the very beginning of the development process.

The second idea is that all the reliable security tools are not the complete solutions. Though, they are great resources in the hands of developers because they mean the reliance on proven protocols and implementations to give systems certain security properties, they are rather incomplete. This means that more high-level tools must be found to create user-oriented solutions.

The third important issue is that security is not something to handle only in the lower layers of the networking stack or in the depths of the operating system. If trying to solve the security problem purely in those lower layers, users inevitably have to deal with those layers when something goes wrong. Therefore, the security mechanisms must be compatible with what the user needs to accomplish.

The fourth recommendation is to put the users' needs first. The information security representatives often believe that security is more important than users' other needs, even when it results in a system that does not let users accomplish the tasks for which that system was designed. So, when designing a system, professionals must keep in
mind that they are not average users, and after they finish the system, their target audience should test it. Such studies can provide the basis for effective iteration cycles of design, implementation, and evaluation.

The last point is to try to think and act locally. Security solutions often seem to require generic, universal answers to problems, which do not actually exist in practice. Systems that follow the "think locally" principle are much easier to deploy, because they do not require administrators to coordinate with some larger infrastructure. As a result, they can offer greater opportunities for automatic configuration.

Conclusions

As the analysis of the publications shows, very few studies have been devoted to finding a balance between security and usability. However, when evaluating the security of a system, this

task is important in order to avoid a skew in the direction of cumbersomeness or weakness of the system. The solutions presented in the article are not a panacea for assessing the security of the system, but they set a new vector for development in this direction and expand the field of scientific and engineering activities in this area.

REFERENCES

1. Burkova E.V. The task of assessing the security of information systems of personal data // Bulletin of the Chuvash University. – 2016. – №1. – P. 113.
2. Alshamari M. A Review of Gaps between Usability and Security/Privacy // Int. J. Communications, Network and System Sciences. – 2016. – №9. – PP. 416-420.
3. Hof H.-J. Towards the enhanced usability of IT security mechanisms // User-Centric IT Security. – 2015.
4. Security and Usability: Analysis and Evaluation / R. Kainda, I. Flechais, A. W. Roscoe. // International Conference on Availability, Reliability and Security. – 2010. – PP. 277-279.
5. In search of usable security: five lessons from the field / D. Balfanz, G. Durfee, R.E. Grinter, D.K. Smetters. // IEEE Security and Privacy. – 2004. – PP. 21- 23.

Scientific and Practical Cyber Security Journal (SPCSJ) 2(2):18-24
Scientific Cyber Security Association (SCSA), 2018 ISSN: 2587-4667

DIGITAL STEGANOGRAPHY AND ITS EXISTENCE IN CYBERCRIME

Natasha Garcia
Utica College, Utica, New York

ABSTRACT

The steganography evolution has been driven by the necessity for hiding a secret communication and eliminating its existence. The communication is conveyed between two parties. As a result, the primary objective with steganography is largely concealing the existence of said communication and protecting the embedded data against any modifications such as compression or format change that may happen during a transmission. As technology is adapting, computer users are seeking opportunities to protect the data they are sending. Digital steganography has had recent exposure due to its use for malicious activity and hiding illegal information across the Internet. The use of steganography online is a new practice and training in the law enforcement field has yet to be fully developed. This paper focuses on the specifications of digital steganography, its involvement in cybercrime, and the training opportunities for forensic examiners and law enforcement.

KEYWORDS: Computer steganography, cybercrime, digital forensics

INTRODUCTION

The creation of steganography has been transformed into the realm of the digital world due to the expansion of computer power, the Internet, digital signal processing (DSP), information theory, and coding theory. Digital steganography has created a climate of corporate cautiousness that has generated various intriguing applications and software; therefore its continuing evolution is ensured. The advancement in digital information has created new challenges for sending information in a secure and safe manner. Whichever method is chosen, the most vital question is its level of security. Various approaches have been created and developed over the years for addressing the issue of information/data security such as cryptography and steganography. This paper outlines the types of digital steganography covers, training opportunities for forensic examiners and law enforcement, and involvement of steganography in cybercrime.

WHAT IS STEGANOGRAPHY?

To understand digital steganography, it is essential to understand the term before its incorporation in technology- steganography. Steganography is the art and science of invisible communication (Sadek, Khalifa, & Mostafa, 2015). The source of the word *steganography* comes from the Greek language. It is derived from two Greek words *stegos* which means "cover" and *grafia* which means "writing" (Sadek et al., 2015). The steganography evolution has been driven by the necessity for hiding a secret communication and eliminating its existence. The communication is conveyed between two parties. As a result, the main objective with steganography is largely concealing the existence of said communication and protecting the embedded data against any modifications such as compression or format change that may happen during a transmission. A fundamental important feature of steganography is perceptual transparency (Sadek et al., 2015).

TECHNIQUES

There have been several methods when discussing digital steganography. However, one of the earliest methods to consider is credited to Charles Kurak and John McHugh, who proposed a method which resembles embedding into the four least significant bits (LSB) (Cheddad, Condell, Curran, & McKevitt, 2010). Both McHugh and Kurak analyzed image downgrading and contamination which is roughly known now as image-based steganography (Cheddad et al., 2010).

More recently in the cyber field, DNA-based steganography techniques have gained traction. The elevated randomness in a DNA sequence can be applied effectively in order to conceal any message or information without being detected. DNA-based steganography has been considered a valuable example of steganographic media, due to its note-worthy storage capacity and the ability to synthesize DNA sequences in any desirable length (Sadek et al., 2015).

Substitution-based techniques replace surplus data of the cover with the intended secret message (Sadek et al., 2015). The primary advantages of the use of substitution-based are the simplistic implementations with the addition of a high capacity for embedding in comparison to other techniques (Sadek et al., 2015). To name a few, substitution-based techniques include several methods such as the most frequent LSB technique, Bit-Plane Complexity Segmentation (BPCS), Tri-way Pixel Value Differencing (TPVD), and many others (Sadek et al., 2015).

LSB technique is one of the oldest and most famous substitution-based procedures. Not only is it simplistic, but it is also capable of hiding large, hidden messages. LSB operates by replacing a few lease significant bits of pixels from a cover video, for example, with the hidden message bits. The secret message is a colored image of dimensions 670×670, and the cover is an audio video interleave (AVI) home video of a child playing. The video has 14 frames each of dimensions 640×480.

STEGANOGRAPHY COVERS

The majority of digital files can be hidden using steganography covers. However, particular formats have been deemed more appropriate than others for this job. To use file formats with a higher redundancy rate, it is important to note the primary goal of any steganographic technique or method; maximize the hiding capacity and to minimize the embedding distortion (Ballard et al., 2016). The redundant bits of a cover object are bits that can be altered without the adjustment being detected effortlessly (Ballard et al., 2016). Established on the type of the cover object, steganography can be divided into five key categories.

Text steganography is a notable method of steganography. Although text steganography is considered one of the more older methods, modern techniques for text steganography include line-shift encoding, feature specific encoding, word-shift encoding (Sadek et al., 2015). In recent years, text steganography has not been used to the extent that it used to. This is due to the fact that text files have an insufficient amount of redundant data which can, in turn, result in an inadequate amount of hiding capacity. Text files are also known to be easily altered which can lead to the secret message being lost.

Due to a high amount of redundant data, images are the most widespread cover objects used for steganography. In steganography, a digital image is seen as a collection of numbers that

represent different light intensities in various areas of the said image (Sadek et al., 2015). There are numerous types of digital image file formats. The most popular ones to note are Joint Photographic Experts Group (JPEG), Bitmap (BMP) format and Graphics Interchange Format (GIF). Although each format is a digital image, they each rely on different steganographic techniques.

Audio steganography is another type of steganography, and it can be viewed as camouflaging in a one-dimensional signal (Sadek et al., 2015). Audio steganography is able to carry out its purpose of hidden communication through the help of the masking phenomenon. This phenomenon suggests that if a loud audible sound exists, a lower audible sound will become inaudible. Examples of audio encoding techniques are phase coding and low-bit encoding.

Video steganography is considered an extension of the digital image steganography. A video stream involves a series of still images that are successive and uniformly spaced. This stream can be accompanied by audio as well. With these factors in mind, many steganographic techniques that are used with images can be applied to videos too. Video files are a favorable type of cover since it can carry a significant amount of data for hidden messages. Although there is more focus on digital images when it comes to steganography, video steganography is starting to evolve due to the repeated use and popularity of videos over the Internet.

Another type of steganography that is worth an honorable mention is protocol steganography. This type of object refers to the implantation of hidden information within a series of network packets. There are hidden channels in Open Systems Interconnection (OSI) network model layers where steganography can be put into place. Steganography can be implemented in the header of the Transmission Control Protocol/ Internet Protocol (TCP/IP) packet to hide data. The idea of retransmission steganography was also presented during a workshop that included a successfully received packet that was intentionally not acknowledged to invoke retransmission (Ahsan & Kundur, 2002). The retransmitted packet carried the secret message as opposed to the original data.

CASES INVOLVING DIGITAL STEGANOGRAPHY

Unfortunately, these object types and techniques can be used for wrongdoing. Cybercrime has proven to be the number one benefit from this digital revolution with steganography. An immediate concern was shown on the possible utilization of steganography by terrorists following a report in *USA TODAY* in 2001 (Cheddad, Condell, Curran, & McKevitt, 2010). The report stated that there was an influx of statements that Osama bin Laden and his al-Qaeda network had been communicating through secret messages on favorable websites (Cheddad et al., 2010). Niels Provos and Peter Honeyman, at the University of Michigan, inspected and analyzed over three million images from top websites looking for any trace of steganography (Cheddad et al., 2010). They were not able to find a single hidden message. Although Provos and Honeyman attributed several reasons for this result, it should be noted that steganography does not exist solely in still images. Embedding hidden messages into video and audio files have also been possible.

In 2010, a Russian spy ring conversed and connected by posting images encoded with secret messages to public websites (Stier, 2010). The Department of Justice (DOJ) recovered over one hundred messages that were concealed within online pictures. These online pictures were then linked to mentioned Russian spy group. After an image containing hidden data was posted online, the receiving Russian party then downloaded the image using steganography software to

interpret it. The spy group posted pictures to the Internet using websites such as eBay and took advantage of the fact that it is difficult to determine who precisely the pictures are for (Stier, 2010). The websites used were public websites that millions of computer users might visit, but only the Russians in the spy group would know that particular images contain hidden data. The numerous amount of pictures on the websites used also made the investigation challenging to find the images that contained the concealed messages between the spy ring.

In June of 2010, the Federal Bureau of Investigation (FBI) detained 11 Russian spies who were using digital steganographic technology to communicate amongst each other stealthily (Bell, 2015). Similar to the mentioned Russian spy ring, these Russian spies used images to communicate and transfer hidden text files. Investigators were able to conduct a search and find the 27-character password the spies were using as well as the steganographic software. Officials found the mentioned password on a piece of paper in one of the suspect's houses. With this discovered password, more than 100 text files were revealed and analyzed. Officials also noted that the spies made another mistake. The steganography software used by the spies were not commercially accessible. The software was developed in Moscow, allegedly linking the spies to the Russian Foreign Intelligence, Sluzhba Vneshney Razvedki (SVR) (Bell, 2015). An investigator stated in the report that the software was easily accessible on the confiscated computers. The steganography software was accessed by pressing *Ctrl + Alt + E* and the 27-character password was then entered (Bell, 2015).

In 2011, a suspected al-Qaeda member was arrested in Berlin, Germany in May. This suspect was he found with a memory card with a password-protected folder. Examiners discovered hidden files were contained in the protected folder. However, as the German newspaper *Die Zeit* reported, digital forensics examiners from the German Federal Criminal Police (BKA) claimed to have eventually uncovered its contents (Gallagher, 2012). The examiners reported that a video was uncovered and appeared to be a pornographic video. Within that video, forensic examiners were able to reveal 141 separate text files (Gallagher, 2012). They claim that the documents contained details regarding al-Qaeda operations and future operating plans. Among these documents were three documents labeled "Future Works," "Lessons Learned," and "Report on Operations" (Gallagher, 2012).

A Russian hacker group named Advanced Persistent Threat (APT) 29, used steganography in 2015 to disguise communication within pictures on GitHub (Bell, 2015). Specific instructions were given to infected machines to check various Twitter accounts. Every time a tweet was displayed, the malware located on the machines would be activated (Bell, 2015). A network security firm by the name of FireEye discovered the malware and a steganography technique the hacking group was able to implement. In their report, FireEye called the malware tool Hammertoss and admitted that hackers have become "more sophisticated with their ways to stay hidden" (Bell, 2015). APT29's tool Hammertoss consisted of several malware techniques as well as steganography techniques to accomplish its laden objectives.

In July of 2002, the European Police Office (Europol) exposed a pedophile group named the "Shadowz Brotherhood" (Wingate, 2006). Members of this group were reported to be concealing obscene material containing children in seemingly innocent image files. Although media outlets did not reference steganography as the main topic of the investigation, officials explained that one or more steganographic applications were used to hide the child pornography in the images and distribute them (Wingate, 2006).

TRAINING

It has been stated that digital steganography continues to find its way in child pornography cases as well as overseas incidents. However, despite the cases such as Hammertoss, the Shadowz Brotherhood, and possibly other cases that have not been the focus of public attention, the question of whether digital steganography is a danger continues to be a paradox. In recent years, the number of computer forensic examiners interested in specializing in digital steganography has decreased due to the fact that it has not been proven to be an immense threat in cybercrime (Sadek, Khalifa, & Mostafa, 2015). In order to continue research and prove that digital steganography is, indeed, a threat, forensic examiners need to have access to digital steganography training and shed light on research and information regarding the topic. Steganography has been used in various formats since the times of ancient Greece. However, digital steganography currently has a relatively low visibility to law enforcement agencies on the frontline (Bell, 2015).

When a case that involves digital steganography arises, managers should be mindful that law enforcement investigators and information technology (IT) staff may not have the expertise that a digital forensic professional could have. Creating training tools and material can be considered daunting. A suggested starting point is to begin the search for major commercial steganography vendors and combine the tools with information from the Steganography Application Fingerprint Database and the National Software Reference Library (Warkentin, Bekkering, & Schmidt, 2008). Whether the training is for law enforcement officials or examiners beginning their digital forensic careers, these sources can provide the proficiency to detect and decipher steganographic data.

It is important to consider that the criminals using digital steganography as a means to commit cybercrime are not to be defined as amateurs. The presence of steganographic software on a user's computer alone could have private or professional consequences. Known IT and Security companies have taken the extra step and offer steganography tools and training to increase exposure to digital steganography.

Digital forensic examiners that are familiar with EnCase have a steganographic application in their forensic workstation. Examiner can import a library or build their own library of hash sets (in this particular situation, a steganography software) with the library feature in EnCase. The hash sets are then used to identify the steganographic file matches (SANS Institute, 2003).

Black Hat offers a digital steganography course for examiners to practice with modern steganographic tools and techniques (Black Hat, 2007). This hands-on course also provides trainees with experience in the latest investigation methods such as analyzing and recovering hidden data in various cover types. Examiners that train with Black Hat will also be exposed to subject matter such as children exploitation, terrorists and criminal organizations that use the Internet as their means of communication, and corporate insiders.

Training courses such as the classes that Black Hat offer students the opportunities to learn detection, analysis, cracking, and recovery of hidden information. In laboratory settings, examiners are introduced to the newest and digital steganographic software where instructors can demonstrate and define their use in today's cases. Other companies such as Backbone Security and Alpine Security, emphasize the need for understanding how video/image data embedding work as well as the concept of TCP/IP covert channels (Warkentin et al., 2008). The training and

tools are present in the digital forensic community, but it is imperative that the opportunities be taken to crack down on digital steganography.

CONCLUSION

Steganography is the science of concealing data within data. Although digital steganography is becoming more progressive, it is still a topic in science that is not well-known. Steganography has a promising future on the Internet and, in turn, may spark the need for additional research and resources to combat it. This argument is the reason why law enforcement officials must persistently stay well-informed in this area of technology; there will always be a new program ready to obstruct their efforts. Law enforcement is not the only ones that are faced with this responsibility. Digital steganography also presents new challenges for security and cybersecurity personnel, enterprise managers, courts systems, and lawmakers. Future research of digital steganography and steganalysis should always be encouraged for both academics and specialists.

REFERENCES

1. Ahsan, K., & Kundur, D. (2002). Practical data hiding in TCP/IP. *ACM Multimedia and Security Workshop*. The Special Interest Group of Multimedia.
2. American Psychological Association. (2013). *Publication manual of the American psychological association* (Sixth ed.). Washington DC: American Psychological Association.
3. Ballard, J., Hornik, J., & McKenzie, D. (2016). Technological facilitation of terrorism. *American Behavioral Scientist, 45*(6), 989-1016.
4. Bell, R. (2015). Digital steganography: Its impact on mobile forensics, hacking, and social media. *ProQuest Dissertations Publishing*, 25-35.
5. Black Hat. (2007). *Discover the hidden – steganography investigation training*. Retrieved from https://www.blackhat.com/html/bh-usa-07/train-bh-us-07-ws-stego.html
6. Cheddad, A., Condell, J., Curran, K., & McKevitt, P. (2010, March). Digital image steganography: Survey and analysis of current methods. *Signal Processing, 90*(3), 727-752.
7. Gallagher, S. (2012, May 02). *Steganography: how al-Qaeda hid secret documents in a porn video*. Retrieved from https://arstechnica.com/information-technology/2012/05/steganography-how-al-qaeda-hid-secret-documents-in-a-porn-video/
8. Sadek, M. M., Khalifa, A. S., & Mostafa, M. G. (2015, September). Video steganography: a comprehensive review. *Multimedia Tools and Applications, 74*(17), 7063-7094.
9. SANS Institute. (2003). *Steganalysis: Detecting hidden information with computer forensic analysis*. Retrieved from https://www.sans.org/reading-room/whitepapers/stenganography/steganalysis-detecting-hidden-information-computer-forensic-analysis-1014

10. Stier, C. (2010, July 02). *Russian spy ring hid secret messages on the web*. Retrieved from https://www.newscientist.com/article/dn19126-russian-spy-ring-hid-secret-messages-on-the-web/
11. Warkentin, M., Bekkering, E., & Schmidt, M. B. (2008). Steganography: Forensic, security, and legal issues. *Journal of Digital Forensics, 3*(2), 17-34.
12. Wingate, J. E. (2006). *Digital steganography: threat or hype?* Retrieved from http://www.infosectoday.com/Articles/digitalstego.htm#author

Scientific and Practical Cyber Security Journal (SPCSJ) 2(2):25-27
Scientific Cyber Security Association (SCSA), 2018 ISSN: 2587-4667

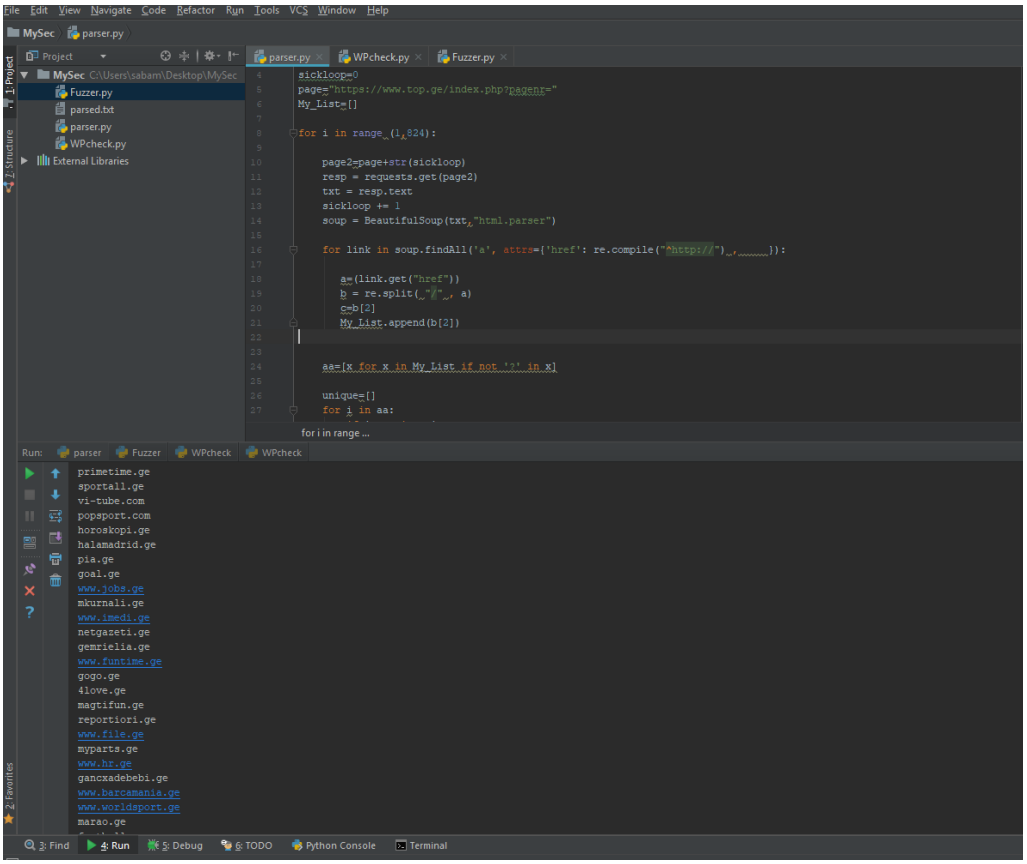
ATTACKS ON WEBSITES WITH INAPPROPRIATE STRUCTURE

Saba Meskhi
Business and Technology University, Tbilisi, Georgia

ABSTRACT

The article concerns the problems of Georgian web developers and cyber security issues related with these problems, that are demonstrated and revealed using testing methods.

როგორ შეიძლება, გულუბრყვილობამ საფრთხე შეუქმნას თქვენს ვებ-საიტს?
განვიხილოთ შემთხვევა როდესაც ადამიანი ტოვებს სახლის გასაღებს აშკარა ადგილას. ქურდს არ აქვს წინასწარი ცოდნა იმის შესახებ, თუ სადაა დამალული გასაღები, მაგრამ შეიძლება ითქვას, რომ თუ ის სავარაუდო და მარტივად პროგნოზირებად ადგილებში დაიწყებდა ძიებას, აუცილებლად მიაგნებდა დაუდევრად გადამალულ სახლის გასაღებს!
კიბერ სივრცეში საიტის ბექაპი აუცილებელია. ასევე აუცილებელია მისი დაცვა [1,2].
დავუშვათ, რომ ჩვენი საიტის ყველა ფაილი ჩვენ მიერ ერთ ფაილში დაარქივდა და დაერქვა, a.zip. ეს ნიშნავს, რომ თუ ვინმე შევა საიტზე - "http://example.com/a.zip" ბრაუზერი ავტომატურად დაიწყებს ამ ფაილის გადმოწერას და კიბერ დამნაშავე ხელში ჩაიგდებს ჩვენი საიტის ბექაპს.
გადავიდეთ პრაქტიკულ ნაწილზე და გავიგოთ, რამდენად მიამიტნი არიან ქართველი დეველოპერები კიბერ ჰიგიენაში.
ამისათვის დავიხმაროთ Top.ge - საიტი, სადაც განთავსებულია ქართული ვებ-გვერდების რეიტინგი.
საიტების დასახელების წამოსაღებად და ტექსტურ ფაილში ჩასაწერად დაიწერა პითონის სკრიპტი.

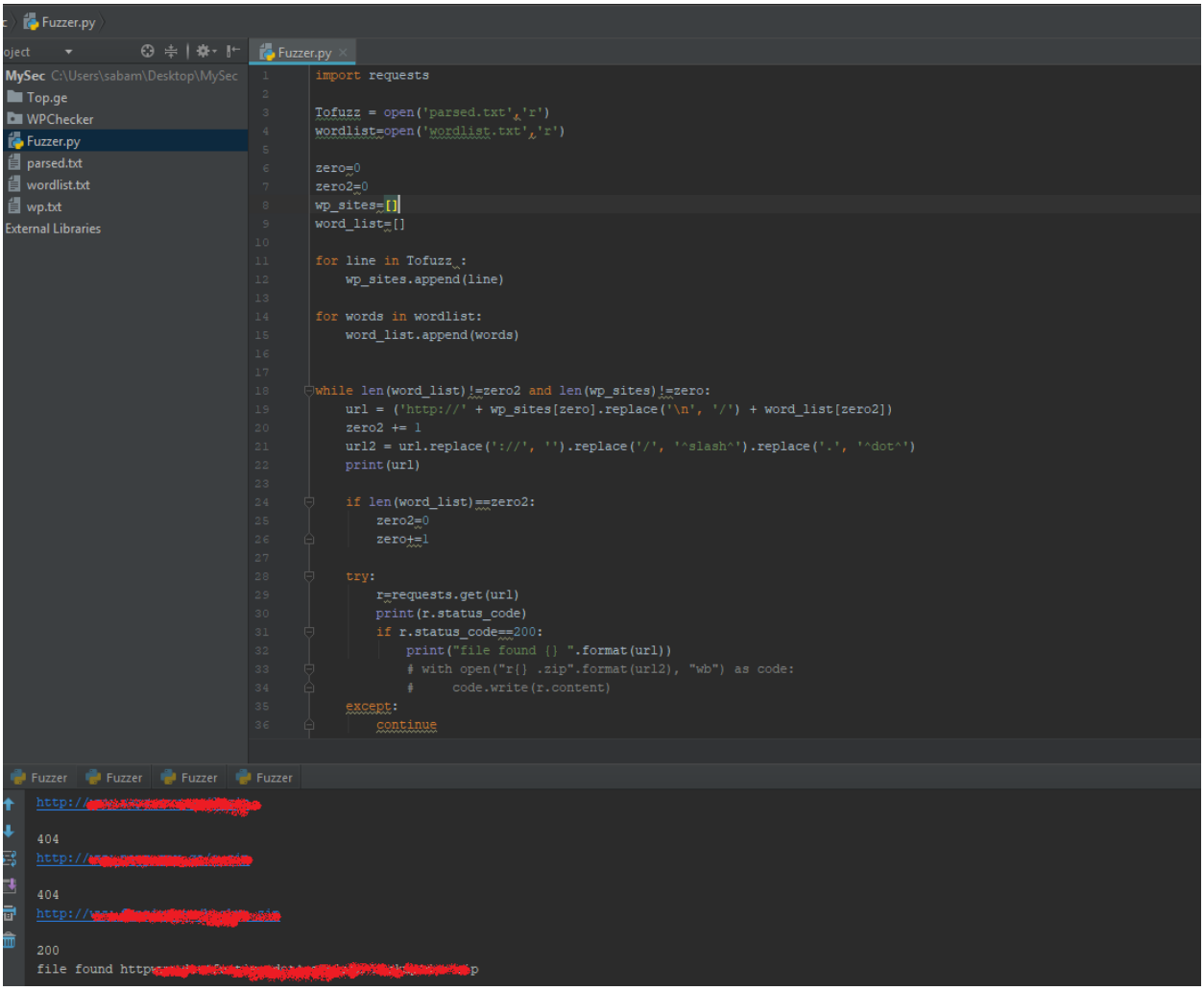


სურათი 1.

სულ გამოვიდა 16000-მდე საიტის დასახელება.
როგორც ქურდმა, ასევე კიბერ დამნაშავემაც არ იცის, სად იმალება საიტის გასაღები , ანუ რა სახელი აქვს საიტის ბექაპს. ამისთვის საჭიროა, ის მოიებნოს მარტივად პროგნოზირებად ადგილებში.
სადემონსტრაციოდ გამოყენებული იყო 4 სავარაუდო დასახელება.

- backup.zip
- backup_old.zip
- 1.zip
- a.zip

დაიწერა სკრიპტი, რომელიც ტექსტური ფიალიდან იღებდა საიტების დასახელებას, და აწყვილებდა სავარაუდო დასახელებებს, ფაილის არსებობის შემთხვევაში კი აბრუნდებდა “200” კოდს.
სკრიპტის გაშვებიდან რამდენიმე წუთში ფაილი, ანუ საიტის გასაღები ნაპოვნია!



სურათი 2.

ამგვარი შემთხვევების თავიდან ასაცილებლად, უნდა შემოწმდეს საიტის დირექციები, ფაილები და მასზე მინიჭებული უფლებები.

REFERENCES

1. Frank McCown , Catherine C. Marshall , Michael L. Nelson, Why web sites are lost (and how they're sometimes found), Communications of the ACM, v.52 n.11, November 2009
2. Frank McCown , Michael L. Nelson, Recovering a website's server components from the web infrastructure, Proceedings of the 8th ACM/IEEE-CS joint conference on Digital libraries, June 16-20, 2008, Pittsburgh PA, PA, USA

Scientific and Practical Cyber Security Journal (SPCSJ) 2(2):28-37
Scientific Cyber Security Association (SCSA), 2018 ISSN: 2587-4667

INTERNATIONAL CYBER SECURITY CHALLENGES AND SCADA SYSTEMS

Tinatin Mshvidobadze
Gori State University

ABSTRACT

The development and application of the information and communications technology has created a new battleground. Cyber security will significantly affect international relations in the 21st century. This paper gives an overview of the concepts and principles of cyber threats that affect the safety and security in an international context.

It is shown the state of the art in cyber security risk assessment of Supervisory Control and Data Acquisition (SCADA) systems. The discussion begins with an examination of what constitutes critical national infrastructure and the roles of ICS and SCADA systems within it. The examination also touches on the political and social challenges in achieving greater cyber security, and then shifts to a description of how the US government divides efforts among its lead cyber security agencies and what responses to a cyber attack on ICS or SCADA might look like. The discussion finishes with recommendations for strengthened international consensus on norms for state behavior, formalized public-private relationships, and interagency efforts to realize a more secure and resilient national infrastructure.

KEYWORDS: cyberspace, cyber-attack, cyber terrorism and crime, international security.

Cyber-attacks on infrastructure

We now live in a world where warfare can be conducted entirely virtually – though the consequences will almost always have repercussions in the physical world.

As we integrate technology further into our lives, the opportunities for abuse grow. So too, then, must the defenses we employ to stop them through the education and practice of cyber security.

AS societies around the world defend ever more heavily on technology, the ability to shut down or destroy infrastructure, take control of machines and vehicles, and directly cause the loss of life has become a reality. To date, some of the more well-known examples of cyber-attacks on infrastructure include:

• In 2008 when Russia sent tanks into Georgia, the attack coincided with a cyber-attack on Georgian government computing infrastructure. This is thought to be one of the first land and cyber coordinated attacks [1].

• Also in 2008, Stuxnet – a computer worm purportedly jointly designed by the US and Israel – crippled Iran's nuclear-enrichment program by sabotaging centrifuges [2].

• In 2014 a German steelwork was disabled and a furnace severely damaged when hackers infiltrated its networks and prevented the furnace from shutting down [3].
• In 2015, with an attack strongly suspected to have originated from Russia, 230,000 people lost power when 30 sub-stations in Western Ukraine were shut down via a remote attack [4].
In all of these, and as an indication of how the landscape of war is changing, the weapon of choice for these attacks wasn't guns or bombs – it was a keyboard.
French Coldwell, Chief Evangelist at governance, risk, and compliance apps company Metricstream, at a cyber-security summit earlier this year noted that "this is the canary in the coalmine. Much more of this will come" [5].
We can expect governments around the world to strengthen their cyber-attack and defense capabilities, spurring an arms race that will operate at a much faster pace than we saw in the Cold War. But here the results could be much subtler – as noted in the McAfee 2016 Threats Predictions report, "they will improve their intelligence-gathering capabilities, they will grow their ability to surreptitiously manipulate markets, and they will continue to expand the definition of and rules of engagement for cyber warfare." [6]

International cyber security

Cyber warfare and terrorism do not know borders. Action in cyberspace requires the rejection of the common assumptions related to time and space because such attacks, by means of modern information and communications networks, can be performed from anywhere in a very short time. The processes of globalization did not have the impact only on the achievements of civilization, but also on the development of new threats to the civilization.
The initial hypothesis is that cyberspace is a growing security risk and challenge of modern times. Moreover, cyber security will significantly affect international relations in the 21st century, while the threats and challenges will exponentially increase.
The scientific work seeks to show cyberspace as an operational dimension of international relations in terms of the cyber security challenges. With the systematization of the cyber warfare strategy and the very methods of attack, links with the planned action will be set up through the application of technical, computing and network systems.
The new, cyber dimension of international relations is a major challenge for the theories of the preservation of power and intimidation. Cyber threats are serious, destabilizing and on the increase. The theories and strategies of intimidation designed and implemented during the Cold War cannot be implemented in the cyber domain. Many scientists are working on the understanding of the cyber revolution in international relations.
Authorities have also taken certain steps in cooperation, especially in the area of crime and the establishment of CERTs (Computer Emergency Response Teams) [7]. Tatalović, Grizold and Cvrtila write that the processes of internationalization and globalization have brought a greater cohesion and efforts for a unified regulation of the world order, more than it was in the system of sovereign states during the Cold War. This is reflected in the core of the states' security policies. In that context, a new concept – human security concept – emerged in theory and political practice. In contrast to the traditional concept of national security, it primarily emphasizes the security of an

individual, not the state [8]. Lin theorizes [9] about cyber security. The concept of intimidation was the basic idea of the nuclear strategy. Even though nuclear and cyber weapons share a key feature – the superiority of the attack in comparison with the defense – they differ in many ways. Experts and analysts estimate that the efforts of Russia and China to dominate cyberspace have over the past few years intensified so much that any delay in this area could present a big problem for the modern West.

Cyber-attack, whether it happens as a conflict between states, a terrorist or a criminal act, is an attack in cyberspace with the aim of compromising a computer system or network, but also of compromising physical systems as it was the case with the Stuxnet worm. In layman's, popular terms, most often mentioned in the media, it is called a hacker attack. Identical methods of a hacker attack are applied for both military and terrorist purposes.

Janczewski and Colarik [10] divided cyber-attacks into phases, which they consider to be basically the same as the phases of conventional criminal offenses:

• the first phase of the attack is the scouting of potential victims. By observing the implementation of the normal operations of targets, useful information that are accumulated and determined through the used applications and hardware;

• the second phase of the attack is intrusion. Until the attacker gets into the system, there is not much that can be done against the target apart from disrupting the availability or access to certain services provided by the target;

• the next phase is the identification and dissemination of internal opportunities by examining the resources and the right to access the restricted and important parts of the system;

• in the fourth phase the intruder does damage to the system or steals certain data.

In such circumstances of transformation and different views and understandings of security in general and international security, cyber threats certainly redefine those terms. In line with the efforts to ensure security on one hand and specificities of cyber threats and motives of the actors who initiate them on the other, it will be necessary to set up a new international security paradigm of the cyber age.

SCADA systems and cyber security challenges

A SCADA system consists of hardware and software components, and of a connecting network(s). Fig. 1 shows a generic hardware architecture of a SCADA system. An architecture is formed by one or more control centers and a number of field devices such as an RTU, Intelligent Electronic Device (IED) and Programmable Logic Controller (PLC) connected by a communication infrastructure. An RTU receives data from field devices, converts it to digital data and sends it to the control centre as well as receives digital commands from the centre and handles alarms. A PLC is a digital computer that monitors sensors and takes decisions based upon a user created program to control valves, solenoids and other actuators. A control centre includes an MTU, which issues commands to and gathers data from RTUs, it also stores and processes data in order to display information to human operators to support decision making.

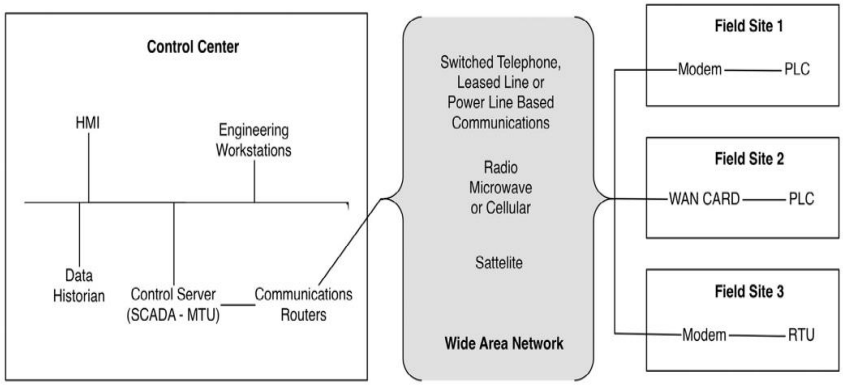


Fig. 1 – Generic SCADA hardware architecture. NIST SP 800-82

In reality, security goals, in whatever order they appear, are often preceded in SCADA systems by safety, reliability, robustness and maintainability (which are the supreme goal of critical systems) leaving little or no resources for security goals. In Park and Lee [11], the authors discuss a need for an update of such well-established international security standards as NIST SP 800-53 and ISO 27001 in order to address the specifics of ISC is stated. A new standard, according to Park and Lee, shall bring together the CIA-traid and safety requirement critical in the context of an ICS.
Cyber security issues in SCADA systems are further exacerbated by the legacy problem. Existing SCADA systems, due to their continuous operation, are not updated or re-designed in some cases for decades. The nature of SCADA systems requires them to be operational 24 hours 7 days a week. This makes the regular patching and upgrading of both a SCADA software and a hosting operating system difficult, if not impossible. The patching of a SCADA system is complicated by the facts that the system is time-critical, there is no test environment and patching may introduce new unknown vulnerabilities or ultimately break the system. Legacy SCADA system may end up relying on operating systems and software that are no longer supported by vendors [12].

Risk assessment methods for SCADA Risk assessment, detection, and response, 2011
A risk assessment method for sensor networks accompanied by attack detection and automatic response modules is presented in Cardenas et al. [13]. In Cardenas et al. the standard formula for calculating risk as an average loss is accepted and interpreted in the context of a sensor network:

$$R_\mu = \sum_i L_i \; P_i \qquad (1)$$

where P_i is the probability of an attacker compromising sensor i and is accepted to be the same for all sensors and L_i is a loss resulting from the compromise.
The following attack model is proposed which may reflect integrity and DoS attacks:

$$\acute{y}_i\ (k) = \begin{cases} Y_i\ (k), & for k\ \notin \mathrm{K}_\alpha \\ a_i\ (k), & for\ k\ \in \mathrm{K}_\alpha, a_i\ (k) \in \gamma_a \end{cases} \quad (2)$$

where $\acute{y}_i\ (k)$ is a measurement received by the controller at time k; $Y_i\ (k)$, is an actual measurement; $a_i\ (k)$, is a measurement under attack; and K_α is the duration of an attack.

For detecting anomaly, a linear model as an approximation of the behavior of a physical system is developed. Then, anomaly is detected using a non-parametric cumulative sum statistic. When anomaly is detected, an automated response to an attack is fired while awaiting human actions. The experiments were run to simulate cyber attacks on a chemical reactor implemented as a Tennessee-Eastman process control system model presented in Ricker [14]. The experiments demonstrated that the risk assessment model proposed helps to establish which type of attack and which sensor in a network must be given a priority in a security budget.

Threat Trends

The opportunities for a cyber attack on SCADAs are replete with various methods and avenues of attack to achieve devastating effects on a target network.

The effects of data manipulation, instrument alteration, or power fluctuation upon an ICS or SCADA systems represent scenarios where cyber generates tangible effect upon businesses or governments. Points of attack may include an ICS, external office IT network, calibration tools, field devices, safety systems, technician support equipment, and even the employees themselves.

The national leadership attention provided to this problem set is directly proportional to the increased public reporting of compromises by both state and non state actors. There have been a startling number of reports recently, including a coordinated cyber intrusion into US pipeline SCADA systems, Russian hackers exploiting Western energy companies and ICSs in 23 countries, Chinese and Russian mapping of the US electrical grid, regional conflicts such as the Syrian civil war bleeding into cyberspace, and unknown hackers shutting down an oil platform by inducing unsafe tilting [15]. There is also growing speculation North Korea could capitalize on known vulnerabilities, and indications that Iranian actors "have directly attacked, established persistence in, and extracted highly sensitive materials from [major] critical infrastructure companies."[16]

Also, several recent and public cyber-attacks on ICSs or SCADAs have generated catastrophic results. The first publicly released and highly formative demonstration of ICS vulnerability was the Aurora Generator Test conducted by the Idaho National Laboratory in 2007, where the intentional and rapid opening and closing of breakers in a commercially available generator induced an out-of-phase condition that effectively destroyed the equipment when connected to the power grid[17].

Security experts extrapolate that the Aurora vulnerability is not merely constrained to generators but extends to electrical systems and rotating equipment elsewhere, such as in manufacturing, refineries, data centers, and mass transit.

In unprecedented official recognition of the threat to SCADA, Adm Michael Rogers, US Navy, director of the National Security Agency (NSA) and commander of US Cyber Command (USCYBERCOM), testified before Congress that "China and 'one or two' other countries are capable of mounting cyber attacks that would shut down the [US] electric grid and other critical

systems."[18]. Any uncertainty in whether the United States appreciates the gravity of this problem set is eliminated in the clearest terms of EO 13636, as "it is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure.

Cyber Response

Cyber responses bearing both challenges and benefits is discussed below. Without considering the means of employment, cyber responses will aim at one or more of the following:

• observe and gain intelligence;
• deny an attack's objectives through defense and hygiene;
• neutralize the attacker and impose a proportional cost on them, or
• retaliate with a high-order response to deter future attacks.

The means of responding could include:

• hacking adversarial command-and-control infrastructure;
• interrupting network protocols;
• luring attackers into honey pot traps;
• coordinating with computer security incident response teams (CSIRT) and Internet service providers (ISP) to disrupt malicious traffic, or
• applying cyber effects to facilities or services, like ventilation or power systems, attackers rely on to execute operations.

Cyberspace is different from other domains in the sheer speed of its activities. Therefore, any related consultative process, such as an emergency national response mechanism, has to be very streamlined and adaptive to respond within an adversary's observe-orient-decide-act (OODA) loop[19]. Additionally, access to and exploitation of "hard" targets in advanced nation-states, might take weeks or months to accomplish. Cross-domain or covert activities might be required before being able to hold adversaries at risk.

Prevention

I consider it appropriate to correct policy recommendations for synchronizing and prevention cyber security efforts.

The first line of effort is prevention, a pre conflict phase where the government can capitalize on the momentum already under way across various sectors and institutions. Prevention also requires complementary foreign and domestic initiatives including:

• international norms of cyber behavior;
• formalized critical interdependencies;
• private-sector responsibilities in law and regulation;
• focused research into advanced cyber capabilities, and
• cyber workforce professionalization.

The United States must strive to establish an international set of norms that define both peacetime and contingency expectations for state cyber behavior, communicate clear cyber foreign policy, pursue cyber defense capacity building measures with developing nations, and develop an international understanding of the nature of "critical infrastructure." Building an internationally

accepted framework of norms of behavior and confidence-building measures in cyberspace are foremost among these efforts. This framework will provide a new level of strategic stability in cyberspace and afford the US government freedom of action in cyberspace consistent with the nation's principles and interests. The interagency approved the draft cyber initiatives on peacetime norms in 2014[20]. The initiatives are intended for future international consideration and hold that states:

• should not perform cyber-enabled intellectual property theft for economic advantage;[21].
• should not attack or impair critical infrastructure;
• should not impede national computer-security-incident-response team actions;
• should behave consistently with domestic and international laws and obligations.

These norms depend upon utilizing traditional multi stakeholder Internet governance rather than state-administered models of cyberspace governance, as the key to an "open, interoperable, secure, and reliable [Internet]." [22].

While such structure implies US unilateral influence may become more diffuse, it reinforces the spirit and character of the Internet.

While the UN and NATO have outlined the initial response frameworks for major cyber attacks, the United States must continue developing and framing adequate prevention measures for the continuous below-response threshold malicious cyber activity that occurs all over the Internet. If network defense and law enforcement mechanisms are not sufficient to mitigate and respond to threats, then the US government will examine cyber, economic, and kinetic options.

The next step involves legislating new mandatory technological, administrative, and personnel standards, as identified in EO 13636, for organizations responsible for critical infrastructure. These entities should:

• formally recognize the NIST Cybersecurity Framework as the defining set of best practices in securing CI/KR;
• participate in the C3VP and ICSJWG;
•undertake DHS-led cybersecurity certification and routine assessment; and
• provide controlled disclosure to DHS of cyber incident forensics.

The federal government should continue to find new and innovative ways to increase sharing of real-time information with critical infrastructure owners while ensuring information classification restrictions do not inhibit the intelligence sharing essential to the cyber safety and resilience.

Threat data must include not only indicators but also the maximum intelligence possible—assuring that it is secure and actionable. Critical infrastructure operators should also have cleared liaison personnel within the NCCIC. That could help eliminate traditional barriers to communication, advocate for rapid declassification of threat intelligence, and ensure that automated information sharing channels like STIX™/TAXII™ are as developed or refined as possible.

DHS should continue developing capabilities to fuse physical and cyber infrastructure situational awareness for a holistic understanding of their interdependencies and potential cascading effects between systems and sectors, for the government and for corporations. DHS should continue to seek and champion ICS and SCADA systems cyber security best practices—such as those developed by ICS-CERT—to provide automatic vulnerability and mitigation recommendations[23] DHS must

also ensure the NIST Cyber security Framework remains as adaptable and dynamic as are the threats to our critical infrastructure. Finally, in the long-term, DHS may consider transitioning the Cyber Security Framework to a nongovernmental entity in the spirit of open and inclusive participation. This might be similar to the gradual shift in Internet governance and oversight from the Department of Commerce to the Internet Corporation for Assigned Names and Numbers (ICANN)[24]. A highly trained and professionalized cyber security corps is the heart of effective cyber security. The DHS should continue to lead and expand cyber security workforce professionalization efforts like NICE. In the same vein, the government should pursue and invest in cyber ranges and simulation exercises. These facilities could promote the integration of DHS, FBI, and DOD experts with ICS and SCADA cyber security staffs to train and exercise skills in a permissive environment with realistic feedback. As General Davis remarked, "[Long-term] institutional capability in cyberspace is about building the right kind of people, including leaders, who truly understand what [cyber] is about, and who can apply the intellectual staying power to secure an advantage for the future."[25].

The federal government must continue to fund and expand the work of the DOE at the National SCADA Test Bed, the leading effort to bring innovation, cyber security, and standards to our critical sectors, which can then be disseminated to private industries. The work conducted within the national labs is the seed corn that will bear true fruit in years to come. From that seed will come key advances in integrated physical and cyber sensor technologies, big data and predictive analytics, trusted supply-chain initiatives, anomalous behavior detection, and secure life-cycle system acquisition and design. However, despite the best layered-security integrating technology with a well-educated workforce, a determined adversary will eventually find an exploitable attack surface and activities must shift from prevention to mitigation.

Conclusions

The topic of the paper, cyber threats to international security, stands out merely by its title as an interesting and challenging area of research. The explanation for it is first and foremost that the area has not yet been sufficiently explored. Due to the intensive development of international relations in cyberspace, conditioned and supported by the speed of the development of technologies and their implementation in the relations of states, organizations and individuals, this area will always be interesting and challenging. That conclusion arises from the constant change of attitudes and technology. It is precisely that instability which indicates that from that specific, interdisciplinary field of research, in 5 or 10 years, it will be possible to draw some new conclusions, and according to them, set some new paradigms and doctrines. Carr states that cyber-warfare has been present for about a decade, but that it is still not well defined. There is no valid international agreement which would establish a legal definition of an act of cyber aggression. In fact, the entire area of international cyber law is still unclear.

The development and availability of information and communications technologies and the ever-present tensions between politically and ideologically different states have conditioned the international relations in cyberspace. Strategic domination in cyberspace has not yet been achieved by any of the entities of international relations. A large number of international entities

demonstrated their presence and willingness to act in cyberspace. That demonstrates a multi polar dimension of cyberspace in which it is very unlikely that domination or bloc division will occur. The reasons lie in the mutual mistrust and fear of espionage in the case of linking the defense systems.
Over the years, we have seen a number of cyber-attacks on SCADA systems. The severity and consequences of attacks vary. Luckily, until now major disasters have mainly been averted. Much of the remaining work is in shaping international consensus on norms of state cyber behavior, enforcing private-sector responsibilities that affect US national interests, and continual investment and effort in refining the interagency leadership in this rapidly changing space. The rise in sophistication and frequency of cyber-attacks, especially against critical sectors, coupled with antiquated and inadequate security practices and the risks from increasing global interconnectivity all demand national unity of effort and international cooperation and consensus to overcome.

REFERENCES

1. Russo-Georgian War, Wikipedia, 2016 en.wikipedia.org/wiki/Russo-Georgian_War.
2. 'An Unprecedented Look at Stuxnet, the World's First Digital Weapon', Wired, November 2014 www.wired.com/2014/11/countdown-to-zero-day-stuxnet
3. 'A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever', Wired, January 2015 www.wired.com/2015/01/german-steel-mill-hack-destruction
4. 'Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid', Wired, March 2016. www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid
5. French Coldwell, Chief Evangelist, Metricstream, National Fintech Cybersecurity Summit 2016, Sydney.
6. 2016 Threats Predictions, McAfee Labs, 2016 www.mcafee.com/au/resources/reports/rp-threats-predictions-2016.pdf
7. N. Choucri and D. Goldsmith, "Lost in cyberspace: harnessing the Internet, international relations, and global security," Bulletin of the Atomic Scientists, vol. 68, no. 2, 2012, pp. 70-77.
8. S. Tatalović, A. Grizold, and V. Cvrtila, Suvremene sigurnosne politike. Zagreb: Golden marketing-Tehnička knjiga, 2008.
9. H. Lin, "A virtual necessity: some modest steps toward greater cybersecurity," Bulletin of the Atomic Scientists, vol. 68, no. 5, 2012, pp. 75-87.
10. L. J. Janczewski and A. M. Colarik, Cyber warfare and cyber terrorism. Hershey: Information Science Reference, 2008.
11. Park S, Lee K. Advanced approach to information security management system model for industrial control system. ScientificWorldJournal 2014;2014:348305.
12.Gold S. The SCADA challenge: securing critical infrastructure. Netw Secur 2009;2009(8):18–20.
13. Cardenas A, Amin S, Lin Z, Huang Y, Huang C, Sastry S. Attacks against process control systems: risk assessment, detection, and response. In: Proceedings of the 6th ACM symposium on information, computer and communications security. ACM; 2011. p. 355–66.
14. Ricker L. Model predictive control of a continuous, nonlinear, two-phase reactor. J Process Control 1993;3(2):109–23. RiskWorld. <http://www.riskworld.net/>. [accessed 16.10.15].

RISI. Industry attacks growing. October 14.
15. Parfomak, Paul. *Pipeline Cybersecurity: Federal Policy*. Congressional Research Service (CRS) R42660. Washington, DC: CRS, 16 August 2012.
16. Tucker, Patrick. "Forget the Sony Hack, this Could Be the Biggest Cyber Attack of 2015." *Defense One*, 19 December 2014. Accessed 8 January 2015. http://www.defenseone.com/technology/2014/12/forget-sony-hackcould-be-he-biggest-cyber-attack-2015/101727/?oref=d-dontmiss.
17. Swearingen, Michael, Steven Brunasso, Joe Weiss, and Dennis Huber. "What You Need to Know (And Don't) About the AURORA Vulnerability." *Power Magazine*, 1 September 2013. Accessed 15 January 2015. http://www. powermag.com/what-you-need-to-know-and-dont-about-the-auroravulnerability/?pagenum=1.
18. Dilanian, Ken. "NSA Director: Yes, China Can Shut Down Our Power Grids." *Business Insider*, November 2014. Accessed 21 November 2014. http://www.businessinsider.com/nsa-director-yes-china-canshut- down-our-power-grids-2014-11?utm_content=bufferbafcd&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer.
19. John Boyd, *A Discourse on Winning and Losing* (unpublished set of briefing slides), document mu43947, 1987, Document Collection, Muir S. Fairchild Research Center, Maxwell AFB, AL; and PPD 21, Critical Infrastructure.
20. Tom Dukes, deputy coordinator for cyber issues, Office of the Secretary, Department of State, to the author, e-mail, 8 August 2016.
21. Daniel, J. Michael, Robert Holleyman, and Alex Niejelow. "China's Undermining an Open Internet: We Must Work Together on Reliable Cybersecurity." *Politico*, 4 February 2015. Accessed February 2015. http://www. politico.com/magazine/story/2015/02/china-cybersecurity-14875.html#.VNYJOJ2opcY.
22. Davis, Maj Gen John A., USA. Keynote Address. Armed Forces Communications and Electronics Association International Cyber Symposium. Baltimore, MD: Defense Video and Imagery Distribution System, 2013. http:// www.dvidshub.net/video/294716/mg-davis-afcea#.VD_u0vlbV8E.
23. .ICS-CERT Advisory (ICSA-11-084-01). "Solar Magnetic Storm Impacton Control Systems," 26 March 2011. Accessed 20 April 2015. https://ics-cert.us-cert.gov/advisories/ICSA-11-084-01.
InfraGard website. Accessed 23 October 2014.
24. Hyman, Leonard. "US to Scale Back Its Role in Internet Governance." *TechCrunch*, 19 February 2015. Accessed 24 March 2015. http://techcrunch.com/2015/02/19/1120736/.
25. Davis, Maj Gen John A., USA. Keynote Address. Armed Forces Communicationsand Electronics Association International Cyber Symposium. Baltimore,MD: Defense Video and Imagery Distribution System, 2013. http://www.dvidshub.net/video/294716/mg-davis-afcea#.VD_u0vlbV8E.

Scientific and Practical Cyber Security Journal (SPCSJ) 2(2):38-58
Scientific Cyber Security Association (SCSA), 2018 ISSN: 2587-4667

VULNERABILITIES OF THE WEB: A SOCIO-LEGAL VIEW

Xingan Li
International Institute for Innovation Society, Helsinki, Finland

ABSTRACT

The purpose of this article is to review the social-legal environment of the emergence of cybercrime. The pervasiveness of information and communications systems brings about a legal gap in regulating the new crimes and new forms of existing crimes. There is also the inevitability for extending the objects that the criminal law should provide shield. The swift progression of technology and the inactivity of legal instruments form a sharp contrast. The multiple roles of computer systems in crime, and the decentralization of the Internet make it more complicated to combat cybercrime effectively through any single measure.

KEYWORDS: Networked society; Universal accessibility; Uncontrollability; Invisibility; Disputability; Divisibility; Low confidentiality; Anonymity; Abuse; Uncertainty of the future

Information and communications systems are producer, container, processor, and transmitter of information. The Internet bears an identity of technological creation and technological concept, under which the connection of computers forms a network, while the congregation of networks forms the Internet (Forcier and Descy 2002, pp. 40-60), being borderless and decentralized, and connecting global computers by Hypertext Transfer Protocol (HTTP). The Internet is merely a wide-reaching congregation of computer networks supported by Internet technology, providing possibilities of mutual communications and of access to information.[1] It does, therefore, not only link machines, but also more importantly "links people, institutions, corporations and governments around the world."[2] Each of the services that the Internet makes available may possibly bring about legal problems, increasing opportunities of cybercrime (Grabosky 2000, pp. 2-3.)

Although countless statistics and empirical studies have tried to depict the development of the Internet, this paper tries to present an illustration of the Internet through such aspects as the increase of Internet users, web sites, Internet hosts, web pages, bandwidth, and the growth of e-commerce. The term "indicator" is used to denote these factors in describing the size of the Internet.

The first indicator is the number of personal computers (PCs) and the Internet users. The scale at which information technology has influenced society can roughly be measured by the proportion of the population with access to computers and the Internet. The primary function of information and communications systems is to process and share information.[3] The more the computers are manufactured, traded and used, to a higher extent will society depend on this intelligent machine. The more the people are connected to the Internet, the greater the share information and communications systems-mediated telecommunications will have for the entire market. In no easy

[1] Reno v. American Civil Liberties Union, Supreme Court No. 96-511, 26 June 1997.
[2] American Civil Liberties Union v. Johnson (Tenth Circuit No. 98-2199, November 1999).
[3] Panavision Intl. v. Toeppen, Ninth Circuit No. 97-55467, D. C. No. CV-96-03284-DDP, 17 April 1998.

way can we count personal computers in use globally, but according to the International Telecommunications Union, up to 2004, there were approximately 772 million personal computers in use in the world (GeoHive 2006). It means that practically thirteen percent of the world population are PC users (ibid.). While the Internet has expanded into 214 countries and world regions, the worldwide Internet users have been increasing fast in the past ten years. in 2007, the global networks of information and communications systems have connected approximately 1.15 billion people (Internetworldstats.com 2007), while in 2015, the number is nearly tripled and reached 3.27 billion (Internetworldstats.com 2015). In 2007, more than one-fourth of them are online Europeans, who have the penetration rate of 39.8 percent (Ibid). In the European Union alone, the 255.58 million Internet users represent an average of more than half the whole population in these countries (Internetworldstats.com 2007). Today, users in Asia constitute nearly half of world Internet population (Internetworldstats.com 2015). The number of European users falls into not more than one fifth (Ibid.). The overall number of world Internet users increased eightfold (Ibid).

As one of the fast increasing fields, Social Networking Services (SNSs) spread in a surprising rhythm into contemporary social life. While the number of users of the SNSs is not available, it was estimated that among Internet users, about 74% of online adults use social networking sites (Pew Research Center 2015). In fact, at present, SNSs are used in a broad range of mobile devices, such as smart phones, cameras, media players, tablets and phablets, and notebook PCs, which are usually connected to the networks when they are in use.

The number of Internet users has a high referential value in measuring the importance of cybersecurity, and the harmfulness of cybercrime. The increase in the number of users represents a transition from non-PC-users to PC users, from non-Internet-users to Internet users, which in turn represents a transition from a lower likelihood of being informed to a higher likelihood of being informed—informed by information of various value orientations: coincident with inherent value notion, or contradictory to it. Problems emerge during the process of personal changes to PC usage caused by the subsequent access to more information and social changes as a result of its members' access to ever-more information.

Suppose the total population constant, the users are fewer than non-users but increasing at a phenomenal rate, while the non-users are more than users but decreasing, a movement from non-users to users. I think of the process as a sandglass. The increase of users is like the flow of sand from the top bulb to the bottom bulb. As to what happens in the sandglass, conflict and crash are inevitable. So it is between users: old users and old users, old users and new users, new users and new users and actually between old users and non-users, and new users and non-users, and so forth. If we consider these users are in different organizational forms, it will become more complex: individual users versus corporate users, and so forth.

Users are not only the subjects in the maintenance of cyberspace order; they are among the potential victims of cybercrime. They may benefit from online activities, and at the same time, they may otherwise suffer losses when targeted by cybercriminals. The figure represents the growth of the online population, which is increasing by a surprising rate compared with population in the traditional society. The citizens in the traditional society do not decrease as the netizens in the cyberspace increase. However, more and more people are obtaining the dual identity as both citizens in society and netizens in the cyberspace.

The crime rate in cyberspace may be low at present. Suppose this rate constant, the absolute number of cybercrime, however, increases along with the growth of the population base of Internet users.[4] Consequently, the number of Internet users is valuable in the calculation of the number and even the rate of cybercrime, in comparison with those figures in traditional society.

On the other hand, given that cybercriminals are also among the Internet users, their growing number and their increasingly extensive geographical distribution indicate the difficulties in cyberspace regulation, cybercriminal detection, investigation, jurisdiction, identification, and conviction, and the costs and effectiveness in crime prevention. The Internet has been expanded to virtually all countries in the world. The Internet contents are using more and more kinds of languages, but with a relative concentration in some main languages, such as English, Chinese, Spanish, Japanese, German, French, Portuguese, Korean, Italian, and Arabic (Internetworldstats.com 2007). People understanding different languages will be more or less Internet-informed, but people who understand the main languages will be more Internet-informed. Therefore, the possible impact of online information on users who understand different languages differs. These numbers and ratios will be constructive in understanding the controllability of the Internet and thus the characteristics of cybercrime.

The second indicator is the increase in the number of web sites, which represents the number of cyber actors, the quantity of cyber resources, the range of services that users can consume, and the number of places that the potential customers can visit. A Netcraft survey in July 2006 found that there were more than 88.2 million web sites on the Internet.[5] From the increasing process of the Internet domain names worldwide, an accelerated ratio of increase can be discovered from the late 1990s.

The primary function of web sites is to serve the Internet users' needs of information resources. It is an important form of information publication, which acts as the counterpart to the traditional printed press. The growth of cyberspace population and the growth of web sites interact with each other. The users include publishers and readers, both of whom can exchange their status with each other. The growing number of web sites accommodates more users, while the growing number of users propels the development of web sites. It is possible that the criminals will be destructive towards the web sites, and in turn, that the users' interests will be damaged thereby. The web sites can also facilitate activities unsuitable for the participation of certain groups of people or the web sites may to publish content unsuitable for certain groups of people to retrieve. Lack of a unified conception concerning whether or not to monitor or censor the use of the Internet may leave this public forum in a status of anarchy and confusion.

In addition, the location of web sites is not the equivalent to in the traditional sense. A web site may exist in several regions or countries simultaneously, including at least in the following possible places:

The location of the web site registration,

The location of the web site owner,

The location of the web site server,

The location of the content author,

[4] Similarly, Parker and Nycum (1984, p. 314) estimated that the volume of computer crime would increase due to the growth in the number of computers.

[5] Netcraft. July 2006 Web Server Survey, 28 June 2006. Retrieved 15 March 2016, from http://news.netcraft.com/archives/web_server_survey.html

The location of the web site manager (webmaster),

The location of the web site retriever,

The location of where the language of the web site is mainly spoken by the native people,

The location of where the web site can mainly be accessed, and where the web site can have an actual influence, etc.

Determination of jurisdiction and harmonization of legislations are based significantly upon these different kinds of locations. The simultaneous involvement of many locations in a single act makes it difficult to select a certain location as the nexus for jurisdiction. The involvement of more locations during the process of information transmission and the complexity of tracing backward pose obstacles for determining the just location. Information and communications systems become an information high sea full of information flow.

The third indicator is the number of Internet hosts. An Internet host denotes a computer connected directly to the Internet; regularly, an Internet Service Provider (ISP)'s computer is a host. The number of hosts is an indicator for the Internet connectivity. As of July 2006, the number of Internet hosts reached 439 million (Internet System Consortium, ISC 2006). From the ISC (2006), the development of Internet hosts from 1969 to 2006 showed that the development was relatively slow in the first two and a half decades, and began to accelerate from the mid-1990s.

A significant aspect of cybersecurity is correlated with the accessibility to computers and networks. Occasionally, these computers and networks are the targets of cybercrime. In these cases, the damaged computers and networks become sources of losses suffered by users. As part of the hardware of the entire Internet, Internet hosts are also important reference factors when considering the prevention of cybercrimes.

The fourth indicator is the number of web pages. As of 2007, the Google search engine collected 8 billion of web sites, indexed nearly 10 billion of distinct web pages, several billion of all types of images: photos, drawings, paintings, sketches, cartoons, posters, and more. It is a complicated matter to correctly provide an accurate quantitative measurement of the growth rate of the Internet. The search engine and web site survey have been regarded as useful ways (Tehan 2002, p. 7). The increase of the number of web pages basically indicates that web-based information with positive value and with negative value is increasing simultaneously. The increase in web pages has had multiple influences on online users. The more the web pages are published, the easier the users can discover the appropriate contents, but the less successful the webmasters can maintain them. The faster the web pages are increasing, the more complicated the situation will be on the part of both webmasters and users in terms of obtaining information, maintaining the contents, and avoiding legal problems.

The fifth indicator is bandwidth growth. Bandwidth measures the capability of the communications channel. Bandwidth growth facilitates more users and more convenient online activities. The lowered cost and enhanced quality of services attract people of various ages, different income levels and educational background to join the online community. A longer online time also becomes possible. Therefore, bandwidth growth directly influences the number of online users, the length of online time, and the categories of online activities.

The sixth indicator is the growth of scale of e-commerce. UN (1997) noted that "an increasing number of transactions in international trade are carried out by means of electronic data interchanges and other means of communication, commonly referred to as 'electronic commerce',

which involve the use of alternatives to paper-based methods of communications and storage of information."[6] Although e-commerce is different from those above-mentioned factors that are directly related to the scale of the Internet, to some extent, nevertheless, we can quantify how many commercial opportunities and interests rely on cybersecurity. That is to say, any cybercrimes that shake the foundation of the Internet will have influences on e-commerce. Direct or indirect, tangible or intangible,[7] pecuniary or non-pecuniary losses can be caused by various kinds of cybercrimes. Therefore, a brief introduction to the growth of e-commerce is not meaningless. At least, in considering the cybersecurity investment and the cybersecurity financing, the scale of e-commerce can be a valuable parameter for making such estimate.

In fact, in the U. S. alone, five years after the introduction of the WWW, the size of Internet economy can compete with traditional sectors, such as energy, automobiles, and telecommunications (Centre for Research in Electronic Commerce 1999, p. 8). The Internet economy also rewrote the history of the employment market (Ibid, p. 9).

Integrity and reliability of information are important for e-commerce.[8] Along with the development of e-commerce, criminals are also transmitting their activities online. The increasing dependence of business on information and communications systems is gradually changing the global social-economic scenario.

In fact, besides e-commerce, many other industries more or less depend on information and communications systems. More people, more assets, and more activities continue to go online, the efficiency of social actions reaches an unparalleled degree on the one hand, the over-dependence on information and communications systems also brings about new risks that society would never have met without the systems on the other hand. It is unnecessary to overemphasize the catastrophic effect of the possible interruption of information and communications systems. However, we should bear in mind that the increasing dependence on information and communications systems would cause more and larger risks for the society. Social disorganization is usually associated with social change, particularly, innovation (Mowrer 1942, p. 32). The information society has the tendency of disorganizing in a more informed way.

The society is transiting from the process of urbanization to cyberization. An information supercontinent is taking shape. The increasing significance of the Internet for society and the accumulated threats of abuse deserve universal attention.

The following sections will analyse the fundamental properties of networked information and communications systems and their primary impacts on the maintenance of social order.

The uncontrollability of networked activities

ICT facilitates free and, frequently, a trans-territorial flow of information. The security of information and communications systems has also been a topic discussed in many literatures from very early years. For example, Bequai (1983, pp. 192-222), and Icove and co-workers (1995)

[6] UN General Assembly Resolution A/RES/51/162 (30 January 1997).
[7] Concerning costs of crime, see Levinson (2002), pp. 336-343, particularly, direct and indirect, tangible and intangible losses of general crime, see Levinson (2002), p. 338.
[8] This kind of recognition makes it imperative for international legal instruments to coordinate position of different countries, for example, Annex to UN General Assembly Resolution A/RES/51/162 (30 January 1997), the Model Law on Electronic Commerce of the United Nations on International Trade Law, Article 8.

covered a wide range of issues connected with computer security. It requires a special forum to provide an answer to the question of whether it is technically, morally, or legally suitable for the Internet to be managed, regulated, or controlled. But a fundamental conclusion is that the security of information and communications systems is only relative. Absolute cybersecurity did not in the past, does not in the present, and will not in the future, exist. Alexander Hellemans (1999) reported that, using a complicated algorithm and software, scientists broke the RSA-155 code, which is a popular means for protecting secret information on the Internet in Europe, even though it is an issue for researchers to spend 5 months on 300 PCs and a Cray 916 supercomputer (p. 1472).

This paper explores the difficulties in exercising control over the Internet. Controllability permits management to exercise a directing or restraining influence over its use, behaviour, and content (Fisher 1984, p. 24). Controllability of the Internet has a direct influence on cybersecurity. The concept of uncontrollability originates from the vulnerability of ICT acknowledged by the pre-Internet writers. Bequai (1978, pp. 9-17), for instance, divided the operation of the system into five stages (input, programming, Central Processing Unit, output and communication process) and asserted that each of these stages is vulnerable to attacks by the perpetrators. Bequai (1983, pp. 4-7) raised four reasons why computer technology is vulnerable: (1) it is vulnerable to abuse, particularly physical attacks and embezzlement; (2) it provides opportunities for various kinds of thefts; (3) it threatens every user with the development of human dependence on the machine; and (4) it functions in a "corrupt environment" where white-collar crime prevails. He concluded that "crimes by computer can be easy" (Bequai 1983, pp. 16-26).

Nevertheless, Kollock and Smith (1999, pp. 3-28) studied "the landscape of cyberspace", and presented a constructive analysis of the social order in the Internet environment. This papper will emphasize and expand the analysis of the security problems usually involved in major Internet services. The characteristics of Internet services with special regard to controllability can be summarized in the following nine respects.

The universal accessibility of the Internet

Universal access to the networked information and communications systems can have both positive and negative roles in terms of social development and social control. Positive, because the society is networked and the networks are available to more and more members of society. Negative, because the traditional social networks have been replaced and the members are moving to and constructing new networks. The impotence of the old order and the absence of the new order will create an integration vacuum, to be expressed in the form of anarchy and chaos, for a process of disintegration and disorganization can be anticipated during this transformation (see Mowrer 1942; Elliot and Merrill 1961).

Since the removal in the 1990s of access constraints on the Internet for commercial use, the premises in which Internet access service is available have been rapidly extended. Besides regular users in schools and companies, cyber cafés and homes also facilitate the access of a significant number of users. In some countries, the management of cyber cafés forms the main path to cybersecurity. Cyber café has become the paradise of school-aged juveniles who play truant. Many problematic youths spend a long time in cyber cafés chatting, gaming, gambling, and entertaining. The cyber café is a place devoid of supervision and restraint as far as both private and public sectors

are concerned. Neither families nor educational institutions can exercise control over activities in cyber cafés. In addition, the owners of cyber cafés are usually motivated by profits and do not care about the users' activities. For instance, many cyber cafés in cities and towns are opened unlicensed due to the failure to meet the requirements of the fire codes.[9] Besides the physical security and Internet addiction, the cyber cafés also involve cybersecurity concerns. Hackers and gangsters are increasingly crowding to the Internet, the cyber cafés being a paradise for them. According to the National Police Agency of Japan, more than half of computer crimes in 2005 were committed by using computer in cyber cafés. An increasing number of Japanese in their twenties and thirties, as well as many homeless people, select cyber cafés, which offer a "bed and Internet" package, as their home.[10]

It is not difficult to comprehend that some Asian countries have outlawed unlicensed cyber cafés. A measure of this kind matches crime prevention and crime control in other countries with a different political situation and cultural background. People from countries without the "cyber-café syndrome" definitely cannot approve such crime prevention measures, and usually protest against governmental actions that shut down cyber cafés. Such protests raise the issue of closing down these premises to the level of a human-rights question. It is then maintained that closure means a threat to information access and freedom of expression. Such a standpoint ignores security and crime concerns. Issues of rights and of crime are always interrelated. It is worth noting that in most European countries, thanks to better living standards, educational and other conditions for the development of a broad bandwidth, the cyber cafés are less developed. The full extent of the issue is thus neglected.

Universal accessibility does not mean that there are no different patterns of usage. People of different ages may spend a different length of time online in carrying out their different goals. People of different gender may exchange different information inside and outside their groups. People in countries in different developing stages may have a different Internet penetration ratio. People are all born equal, but equality of access to information has not been achieved, and equality does not mean sameness. Some people do not want any more information. The impact of information and communications systems on different individuals, groups, organizations and agencies is, therefore, one of different styles: beneficial or harmful, positive or negative.

The invisibility of cyberspace

Conventional countermeasures and theories about crime prevention were based on its material influence and on the material environment, although non-material factors have long existed, too. Activities in information and communications systems can be expressed in a physically invisible form. What are physically visible in information and communications systems are those physical existences, such as hosts and terminals, displayers, keyboards, mouse, and cables, while the mechanisms by which the computers function are invisible. Cyberspace is developed from information and communications systems as an abstract space, differing from the material devices

[9] Lu, L. Online Survivors in China, 13-20 April 2006, Beijing Review.
[10] Konstantin Kornakov, Cyber Café –or the Scene of Cybercrime, 5 March 2007. Retrieved 15 March 2016, from http://www.viruslist.com/en/news?id=208274049.

of information and communications systems that include terminals and cables.[11] It is invisible and intangible if compared with traditional space (Khosrow-Pour 1998, p. 440; Robertson 2000, p. 248; Dodge and Kitchin 2001, p. 81). When a web page is surfed, what can be seen is only the display of information on the screen. The web site is not physically a reading room where people can read magazines, newspapers and books, listen to audio records or watch videos, nor a marketplace, bank, street, or forum. It is merely a collection of web pages written in various mark-up languages, comprised of letters, numbers, and symbols in common use, but which facilitate the functions of linkage to other media, communicating with other people or directing to other services. The electronic address is not necessarily located along a street, in a building or even in a city, province, or country. In addition, the online services are usually provided in the manner of a remote transaction paid by means of digital cash or virtual money. Finally, the Internet users include individuals and institutions, but they do not necessarily appear in person or in an entity in a traditional library, forum, marketplace, bank, or along a street. It is entirely an invisible community in an invisible space.

The low controllability of the process

Since the early days of the computer and the Internet, efforts have not been lacking to control the system. Theoretically, the Internet can be controlled; however, actual and perfect control is unattainable. Thus, it is reasonable to say that the Internet can be controlled by any of the users if there is anyone trying to exercise control over part of it; but it cannot be controlled by any of the users if they want to exercise absolute control over the whole system. The low controllability by one means, on the other hand, the high possibility of control by many others. The low controllability by authorized users means the high possibility of control by unauthorized uses.

According to Kollock and Smith (1999, pp. 3-28), the Internet services have a very low controllability, even though it does not in my opinion greatly affect the social order. They explained the mechanisms of e-mail, Usenet, and WWW, which are the commonest means of communications and information exchange between online users. Both free and paid services are available online on an immense scale. E-mail lists, Usenet, and WWW are used to distribute messages simultaneously to all the subscribers of the lists or Usenet, or published for public access. To some extent, owners, administrators or servers of e-mail lists, Usenet and WWW have a certain degree of controllability when owners decide publish or refuse the messages. However, the openness of most e-mail lists, Usenet and even WWW enables users from everywhere to publish messages. To review a substantial quantity of messages requires considerable time and labour. What makes it a challenging social space is that any online users can write, publish, retrieve and save the contents, meaning that they expose themselves to anonymous users and trans-territorial users (see Kollock and Smith 1999, pp. 3-28).

Kehoe (1993) has discussed the situation of Usenet. He has claimed that the Usenet is not an organization, devoid of central authority; not a democracy, because democracy also requires organization; not fair, because unfair things will be discontinued by no one; nor a public utility, because of little or no control (pp. 36-38). Kingdon (1994) concluded that the Usenet control ends at the newsgroup level rather than at the individual level. Messages can be distributed among

[11] See description in Gibson (1984), etc.

thousands of computers worldwide, and the establishment of jurisdiction over disputes and offences is impossible.

Controllability of online instant messages is yet lower than the above-mentioned services. During the instant communication, the sending and receiving of the messages happen in a nearly synchronous manner. If these messages contain offensive contents, or hyper links to an offensive web page, there is no *sure* way of providing prearranged measures for precluding them. There do exist certain kinds of filtering and blocking mechanisms, but it is still a problematic matter whether these mechanisms are effective in passing and blocking the exact messages. While the filtering mechanisms are based upon logic coding under the hypothesis of rational human activity, the ways in which filtering and blocking programmes can be rendered invalid are simple and multiple. For example, the substitution of letters by similar numbers or symbols, or use of icons as words and phrases, is a method that is easy to use but difficult to filter.

Even if it is merely an individual e-mail, it is still confronted with uncontrollable threats. Kelly (2002) has mentioned the three primary aspects, that is, the loss of the confidentiality of e-mailed information, the distortablity and misinterpretation of content and the possible liability of an institution for the message as a publication.

The above analysis enables us to draw the natural conclusion that the control over the process of the Internet services is theoretically possible but practically unfeasible. The impossibility of control over the Internet immunizes individuals and institutions from any liability for the omission of such a control. Under these circumstances, neither an *ex ante* obligation nor an *ex post* liability can be adhered to as far as related individuals and institutions are concerned. Thus the incentive for control will hardly be strong.

The disputability of content and activities

The old and new diversity between cultures, societies and laws has not necessarily been diminished by the common networks of information and communications systems. On the contrary, universal information and communications systems bring in a diversity from offline to online, and bring about a diversity between offline and online. For example, we see that while there are different versions of religious classics on the networks, there are also different versions of political works online. People have the equivalent chance to read various versions of holy books. If they are to establish a belief different from their previous ones, they are equally likely to be influenced by this version or that version. Thus, from the viewpoint that information and communications systems form a space accommodating different cultures and ethnicities, we cannot expect too much of them, because they have the power both to create and to some extent eliminate diversities. The connection of the Internet to current legal frameworks, including restrictions on displaying unfeasible materials, the protection of privacy, and the limits of permitted business all become the subject-matter of major legal argument.[12] This has become a well-established conclusion.

The capacity of an uncomplicated publishing process makes the web pages an important media for businesses and individuals wishing to convey information to almost as many people as possible (Williams 2001). Every online user is able to contribute to certain kinds of publications: scholars shift their academic journals to inexpensive and easy-spreading digital versions; students

[12] Citron and Toronto Mayor's Committee v. Zundel, 2002 CanLII 23557 (C.H.R.T.).

put their essays on the bulletin-board system; and dissidents establish web sites to publish statements against the political authorities. In addition to technological problems, online content also involve two aspects of legal problems: the protection of free speech in some countries and the prohibition of offensive speech in some other countries. Freedom of speech or freedom of opinion and expression is provided as basic human rights in international agreements and domestic constitutions.[13] Many countries have similar clauses in their constitutions. Although the literal wording in the constitutions may be similar, the judgment standards of free speech are different. What is visible is only the wording of the clauses, but what is invisible is their legal spirit. In some countries, the law of free speech protects online messages, and refusal of publication requests and deletion of published messages may bring about legal disputes. In some other countries, these messages may be legally or religiously offensive. Even within one country, there is also the possibility that the courts rest on positions different from each other or different from the relevant legislation. For example, in Reno v. American Civil Liberties Union,[14] the court struck down a federal provision prohibiting the ending or displaying of obviously disgusting material in a style available to anyone less than eighteen years of age. The court ruled that the prohibition violated the First Amendment.[15] In Ashcroft v. Free Speech Coalition et al.,[16] the Supreme Court of the U. S. upheld the Child Pornography Prevention Act of 1996 (CPPA), which expands the federal prohibition on child pornography to both pornographic images made using actual children and "virtual child pornography."

These factors determine that controllability of the Internet, the legal foundation of control, the willingness to control, and actual control over the Internet are conditionally dependent. Under such circumstances, it is not groundless for technological supremacists to suppose that the Internet lists will assist in the realization of their anarchist ideal.

For example, with the help of the Internet, the pornographic economy has developed on a great scale. It is true that obscene texts, graphics, and audio and video files have a different status in different cultural contexts. They may be legal for all people. They may also be illegal for all people. However, in most cases, they are legal for adults, but illegal for juveniles. In addition, the content of obscene files does not matter: description or illustration of children often render the whole file illegal, because this is regarded as sexually exploiting children. In any case, if the file is illegal, acts with the intent to create, record, possess, present, publish, replicate, disseminate, trade, advertise and so forth are all illegal. Even collecting and enjoying them by oneself will be

[13] In The Universal Declaration of Human Rights 1948, Article 19 prescribed that "Everyone has the right of freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive, and impart information and ideas through any media and regulations of frontiers."

Other primary international agreements including freedom of opinion and expression are The International Covenant on Civil and Political Rights, Articles 19 and 20; The International Convention on the Elimination of All Forms of Racial Discrimination, Articles 4 and 5; The American Convention on Human Rights, Article 13; The African Charter on Human and People's Rights, Article 9; The European Convention on Human Rights, Article 10; The European Convention on Human Rights, Article 10, etc. For more information, see Lawson (ed. 1996).

[14] Reno v. American Civil Liberties Union (Supreme Court No. 96-511, 26 June 1997).

[15] Fallon (2004), p. 53. The First Amendment was implemented in 1791 prescribed that "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."

[16] Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002), Docket No. 00-795 - April 16 2002.

punished. According to the Penal Law of Finland, dissemination of the depiction of obscenity, possession of obscene pictures of children and unlawful marketing of obscene material are all criminalized.[17] However, that the incentive of benefiting from the commercial transaction of pornography motivates the Internet content providers or Internet users means that it is difficult to control the Internet content.

In addition to the fact that the digital form of traditional verbal, written, printed, audio as well as video content inherits these above-mentioned traditional prohibitions, the Internet further inherits the problem enforcing the illegal nature of some activities, such as gambling, along with the trade in some materials, such as drugs, philtres, and weapons. Some of these fields are in dispute. The most controversial issue may be the criminalizing or legalizing of gambling and marijuana. The momentousness of these topics in contemporary society has attracted the attention of multitudinous studies and research. Now, despite their legal status in different countries, exchange of information about these activities and materials, transaction and payment, necessary offline delivery of goods, and possible internationally prohibited money transfer in some areas, may create unsolvable problems for control over the Internet.

Information and communications systems can accommodate contents of different value-orientation and activities of a differing legal nature, usually creating controversies among the various jurisdictions. As a result, the authorities in the country where the content or activities are legal cannot provide sufficient protection for people who publicize legitimate speech or carry out legitimate activities, and cannot prohibit infringements and impose sanctions on people who infringe these legal rights. Similarly, authorities in a country where the contents or activities are illegal cannot impose sanctions on people who breach the proscription, and cannot protect people who obstruct the illegal contents or activities from wrong prosecution by a country where people adopt contrary standpoints to the legal nature of these contents or activities. In Europe, this dispute exists in the respect of speech concerning the identification of several historical incidents, such as the genocide of certain races, denial of which may induce criminal prosecution in countries including Austria, Belgium, the Czech Republic, France, Germany, Italy, Lithuania, the Netherlands, Poland, Romania, Slovakia, and Switzerland. Denial of the historical occurrence of genocide is also punishable in Israel.[18] In spite of some international conventions, the problems of this paragraph are not in practice more easily dealt with than the problems of the proceeding paragraph.

The divisibility of digital files

Division is a threat to most forms of life and most forms of existence. However, at the same time, division means life and the existence of digitalized information. Digital files exist in information and communications systems and are transmitted through the networks in particular forms. Erol (1992) described it as a process of "moving bits from one place to another" (p. 19). In transmitting processes, a file is regularly broken into many packets conveyed along the networks in different jurisdictions. For example, if a European user sends a message from his or her room to the

[17] Penal Code of Finland, Chapter 17, Sections 18-20 (563/1998).
[18] Wikipedia, Holocaust Denial. Retrieved 15 March 2016, from http://www.wikipedia.org/wiki/Holocaust_denial

neighbouring room, the message may be divided into several packets. When they are transmitted from one room to another through the Internet, there is the possibility that all packets are transmitted directly through local networks and arrive at the destination. Nevertheless, there exists, too, the possibility that certain packets transmitted to North America, and then to Africa, or Asia at last arrive in the neighbouring room. It is a frequent phenomenon for a single e-mail message to traverse countries in different continents. If every country attempts to exercise jurisdiction, the process can become exceedingly complex and unmanageable. Plainly put, it may occur that one particular country may simply be crossed by certain packets.

Most of the Internet services involve some kinds of file transmission. For example, contents of e-mail, Usenet, chat room, and web page are generally transmitted as files and divided into packets during the process. Different packets may be transmitted via different routes and different jurisdictions. Even though in reality information is not divided as extremely as we imagine, the possible gap and overlap of legislations have still become a major problem.

The low confidentiality of information and communications systems

Protected data in information and communications systems should be "obtained and processed fairly and lawfully."[19] Technical and organizational measures should be taken to protect personal data against access without authorization, manipulation, disclosure, transfer and other processing without legal reason.[20] Besides general protection of personal data, sensitive personal data are granted special protection by law.[21] Exceptions are derogations,[22] which are prohibited to process.[23]

Information and communications systems are usually analogous to a place with unrestricted freedom and where the information is less confidential. Weak technical control and weak human control are the main factors that expose the weakness of the systems. The most obvious example is e-mail. The technical mechanisms demonstrate that e-mail has exceptionally low confidentiality, and is more vulnerable to disclosure than traditional letters. Without encryption, every document sent by e-mail is publicly accessible, and system administrators can easily view every outgoing and incoming e-mail without any preceding authorization (Sikorski and Peters 1999, p. 348). Kelly (2002) mentioned that the confidentiality of e-mailed information can be lost in such cases as when it is intercepted, when it is sent to a wrong address, or when it is read by an unauthorized or unintended person.

In addition to less prepared gaze, Rogers (2001) worried that the governmental agencies, business organizations and other individuals are usually motivated to abuse their powers and rights

[19] Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Article 5; Directive 95/46/EC, Article 1 (a).
[20] Convention Article 7; Finnish Personal Data Act 523/1999, Section 32 (1).
[21] According to Finnish Personal Data Act 523/1999, Section 11, sensitive data include data relating to or are intended to relate to the following aspects: "(1) race or ethnic origin; (2) the social, political or religious affiliation or trade-union membership of a person; (3) a criminal act, punishment or other criminal sanction; (4) the state of health, illness or handicap of a person or the treatment or other comparable measures directed at the person; (5) the sexual preferences or sex life of a person, or (6) the social welfare needs of a person or the benefits, support or other social welfare assistance received by the person."
[22] Finnish Personal Data Act, Section 12.
[23] ibid, Section 11.

to infringe e-mail privacy. The secrecy of individual interaction in sending and receiving e-mails online is easily destroyed, because of being unencrypted. It is possible for hackers to tamper with the e-mail, or for the Internet service providers (ISPs) to check the packets, resulting in loss of users' e-mails and disclosure of individual privacy or business secrets. This is no different from clandestinely opening other people's letters, encroaching upon other people's correspondence secret (Wang 2001, p. 154).

Computer processing enables "interceptions to be multiplied a hundredfold and to be analysed in shorter and shorter time spans."[24] The interception of electronic correspondence has been legalized under different conditions in many countries. For example, according to the U. S. Electronic Communication Privacy Act (ECPA),[25] ISP may supervise or intercept e-mail information for normal commercial goals and in order to protect property or related right. In addition, in the workplace, it is deemed that the employees have no privacy in company computers.[26] Apart from legally authorized interception, infringement of privacy also poses a great concern.

In fact, many court decisions in the U. S. have rejected the expectation of workplace privacy. At workplace, employers and governments provide information and communications systems for work-related use only. Law and policy limit any use for non-work functions. The logic is that the use of information and communications systems for non-work purposes is a breach of law and policy and deemed misconduct; then, the search into the personal use of these systems does not breach the privacy rights of their employees.[27]

The mobile networks are as vulnerable as the traditional computer networks. Security loopholes usually threaten individual rights and state security. According to the Finnish government news, a serious data security problem has been discovered in the Finnish Ministry of the Interior. With this kind of problem, it became possible to listen to the mobile phone calls of thousands of employees without authorization. Consequently, the Ministry had to inform the employees not to use mobile phones for confidential aims. The problem concerns employees in the police and rescue forces, emergency services, the Border Guard, the Directorate of Immigration, the Population Register Centre, and employees within the Ministry of the Interior itself.[28]

Anonymity

[24] Malone v. The United Kingdom - 8691/79 [1984] ECHR 10 (2 August 1984).

[25] 18 U.S.C. §§ 2510-2522; and 18 U.S.C. §§ 2701-2711. The Act amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the Wire Tap Statute).

[26] For example, in United States v. Ziegler (No. 05-30177 D. C. No. CR-03-00008-RFC ORDER AND OPINION, 6 March 2007), the government argued that:

"Society could not deem objectively reasonable that privacy interest where an employee uses a computer paid for by the company; Internet access paid for by the company, in the company office where the company pays the rent…This is certainly even more so true where the company has installed a firewall and a whole department of people whose job it was to monitor their employees' Internet activity." (p. 1087)

[27] See United States v. Wesley George Thorn, No. 03-3615, Federal Circuits, Eighth Circuit (July 13, 2004); United States v. Angevine, 281 F.3d 1130, 1134–35 (10th Cir.); United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000), etc.

[28] Finland Government News, Data Security problems in Ministry Mobile Phones, 15 February 2006. Retrieved 15 March 2016, from http://e.finland.fi/netcomm/news/showarticle.asp?intNWSAID=47840

The disappearance of physicality in activities on the Internet symbolizes the new way for daily routines, and presents a chance for new practice and changes in faiths, positions, and manners (Zigrus 2001, p. 171). To a certain extent, Internet services are provided for every user who owns a computer and a modem or cable linked to the server. The real identity of the user is not necessary for using the Internet. That is to say, a high degree of anonymity is achievable. Anonymity could indicate an intention to lie or not, to do something deceit or not. In the environment of online communications, particularly during interaction between remote strangers, information and communications systems provide the possibility of maintaining anonymity, and we found that the users of information and communications systems have the willingness to stay passively anonymous, not necessarily actively lying to their counterparts.

In the case of e-mail, it is uncomplicated to register an e-mail account with false information, or to send messages in the name of a certain person. These e-mails may not only infringe the legal rights and interests of the person of the counterfeited identity, but also are able to fabricate a rumour, slander other people, harm other people's reputation, or practise unfair competition to reduce the competitor's trustworthiness. No obligation of free e-mail service providers has been established to investigate the registrants' identity information. In addition, some web sites also provide anonymous e-mail services or sell anonymous e-mail software. [29] Under such circumstances, the traceback of the real sender is impossible. Only where the providers' status is clear, under vicarious liability, can it be useful for law enforcement in some jurisdictions to hold the re-publisher responsible for the content of the original author (Edwards and Walde, eds. 1997, Part 4).

E-mail has frequently been abused in an anonymous way so as to realize a fraudulent scheme. This anonymity not only facilitates a lie, but may also support a fraud. In R. v. Mastronardi,[30] the accused, met the plaintiffs through an Internet dating service, during which the accused misrepresented himself as a single person and engaged in relationship with several victims. He represented himself as:

"(a) coming from a large, powerful and wealthy Sicilian family;

(b) being a widower seeking a wife;

(c) being a medical doctor with a specialty in gynaecology;

(d) having hospital privileges and a clinic;

(e) being a kind, caring and considerate person with positive family and moral beliefs, conveyed in conversations that went on for hours on end;

(f) having elaborate and sometimes bizarre family and cultural traditions requiring highly submissive wives and amalgamation of finances to an account controlled by him;

(g) as time went on, being third in command in mafia like family organization;

(h) not wanting to date, but wanting to immediately enter into an intimate relationship, after which his culture and family regarded them as married;

(i) once so married, his family required him to follow family and cultural traditions." (paragraph 4)

In R. v. Farkas, the accused engaged in online fraud by using different e-mail addresses, mailing addresses, and user names, victimizing sellers and purchasers distributed in the U. S.,

[29] Examples of such services and software can be searched out with search engines.
[30] 2006 BCSC 1681.

Canada, and England.[31] In R. v. Reynolds & Ors, the accused engaged in online chat claiming himself to be a 16-year-old boy, attempting to make young girls expose their bodies and transmit photographs to him over the Internet.[32]

There are many ways by which people make efforts to detect lies, usually including various clues to emotion that may disclose the situation of lying (Ekman 1992, as cited in Howitt 2002, pp. 251-253). However, in the electronic lie, none of the clues can be useful, particularly those emotional ones, because there is no face-to-face interaction. Rather, the interaction itself is covered by a human-machine-human fig leaf.

Another field where people usually maintain anonymity is interaction in chat rooms. Accounting for a considerable fraction of the income of the commercial online providers, chat systems support synchronous communication, discussion on different topics, trans-territorial relationships on common interests, and ignorance of social status (Internet Crime Forum IRC subgroup 2001, pp. 7-9; Rowland 1998; Wilbur 1997, p. 5.). The biggest advantage of the interaction in chat rooms is that the user can keep anonymous at the beginning of the chat or remain anonymous during the whole process. Keeping anonymous means that people are able to fabricate identities that cannot be used to identify them. By disguising themselves, users can perpetrate fraud and many other related activities. This approach is definitely useful, too, in detection and investigation of crimes, where law enforcement uses falsified identity to allure and arrest suspects.[33] The actual reality is that, in information and communications systems, determining users' identity proves difficult, but not impossible.[34]

The abuse of services

The powerfulness of the Internet facilitates instant communication and timely information exchange, covering an unlimited range of messages and information, desirable or undesirable, legal or illegal, beneficial or anti-social. The convenience of e-mail for communications is frequently exploited as the fastest and easiest ways of spreading computer viruses, spam, and frauds over the Internet.

The e-mail is the primary means for spreading malicious programmes. For example, the Love Bug virus reached millions of computers within 36 hours of its release from the Philippines thanks

[31] 2006 ONCJ 121, 10 April 2006.
[32] [2007] EWCA Crim 538 (08 March 2007).
[33] For example, in United States v. Helder (Eighth Circuit, No. 05-3387, 16 March 2006), an undercover officer used a screen name and claimed to be a 14-year-old girl to entrap the perpetrator (pp. 2-4); in United States v. Baker (Seventh Circuit, No. 05-2499, 24 January 2006), an undercover officer used a screen name and claimed to be a 14-year-old boy to entrap the perpetrator (pp. 2-3); in United States v. Antelope (Ninth Circuit No. 03-30557, 8 June, 2004. Docket num. 03-30334, January 2005), the accused joined an Internet site advertising "Preteen Nude Sex Pics" and started corresponding with an undercover law-enforcement agent, in respect of whom the accused was entrapped when he ordered a child pornography video over the Internet; in United States v. McGraw (Tenth Circuit No. 02-1407, D. C. No. 01-CR-426-B, 2 December 2003), the accused was also caught by an undercover agent, with whom he expressed his interests in "having sexual contact with 'white males between the ages of 12 and 15'," and arranged a encounter. See also R. v. Randall (Provincial Court of Nova Scotia 2006 NSPC 19, No. 1538177, 28 April 2006).
[34] As Peter Steiner's cartoon saying that "On the Internet, Nobody knows you're a dog." Originally appeared in The New Yorker, volume LXIX, number 20, 5 July 1993, p. 61. Retrieved 15 March 2016, from http://www.unc.edu/depts/jomc/academics/dri/idog.html

to e-mail. Subsequently, these malicious programmes can send messages, collect information, delete data, spread a Trojan horse, or plan future accidents (Sadowsky and co-workers 2003, p. 48). At the same time, e-mail bombing, that is, sending a large amount of e-mails to the victim, can crash the victim's e-mail account or servers (Syngress 2002, p. 325). Therefore, a security concern is closely related to e-mails.

The e-mail is both the means and the target of spam, utilized primarily for commercial, political, malicious, or illegal schemes. As a marketing and communications means, e-mail has been gradually abused. Recipients of unsolicited e-mails have to spend much time to deal with messages, wasting human resources and baffling the receiving of useful messages. The sending of bulk mails also consumes network bandwidth and interferes with the ordinary communications service. In addition, unsolicited commercial mails are usually sent anonymously or with a fabricated identity, and the recipients cannot stop subsequent messages. Messages of this kind also include false or misleading headers, deceiving recipients to retrieve messages that they do not want. Moreover, the recipients have no way of expressing their wish not to receive such messages, and have no way of requesting compensation even if they suffer loss. The abuse of e-mail has become a public nuisance in the online environment. Although the use of anti-spam services and technologies is increasing, the scale of spam is continuing to increase as fast (OECD 2004, pp. 2-3; OECD 2005, p. 6), becoming a problem not only for personal e-mail accounts, but also for corporate accounts. In regulating the legal problems which the e-mail brings, traditional criminal law has insufficient coverage.

Cyberstalkers also abuse the e-mail service by sending text-, graphic-, and audio-based messages of a threatening, alarming, or harassing kind to the e-mail account of the intended victim (D'Ovidio and Doyle 2003, pp. 10-17). At present, it is also possible for a video-based message to accomplish the equivalent effect. Other Internet services can also be exploited by cyberstalkers to harass other users, either directly or indirectly. An example of direct harassment can be found when stalker sends harassing messages to a targeted victim. An example of indirect harassment can be found when a stalker uses the Internet communications to obtain a potential victim's personal information, such as a home address etc., and then uses the information to contact by other means. In these cases, children are frequent victims (Internet Crime Forum IRC subgroup 2001, p. 11).

In many incidents, what has been revealed is "the all too common failure of both public and private sector organizations to ensure that safeguards are identified and diligently implemented throughout organizations."[35] Due to the abuse of online services, it can be said that, on the Internet, the use and abuse of the services grow hand-in-hand; and chances and challenges exist simultaneously.

From information society to mobile society: the uncertainty of the future

In the technological field, what is certain is the tendency of ceaseless advancement, but what is uncertain is the outcome of this ceaseless advancement. ICT is the most dynamic field in the present world. Network technology is one of its relevant aspects. In addition to the traditional

[35] Sale of Provincial Government Computer Tapes Containing Personal Information, Re, 2006 CanLII 13536 (BC I.P.C.).

networks, mobile and wireless networks have been developing rapidly in recent years. The goal of the new network technology is to integrate the known advantages of the previous network, avoiding the known disadvantages, while creating the unknown advantages. The most advantageous characteristic of all the networks is the decentralized structure, without central control. The unique advantage of mobile phone and wireless networks is the possibility of wider spatial separation between terminals and network devices. Controllability of such networks is being transformed into new forms. At the same time, the existing security concern has also been transplanted into the new media (Karygiannis and Owens 2002, pp. 21-22). The future of technology and security are unforeseeable.

Computer networks form an uncertain phenomenon with which the legal system should keep pace. In the last few years, people in the U. K. were fond of quoting an estimate according to which the U. K.'s currency reserves can be transferred outside the country in fifteen minutes Kelly 2002). Both the convenience and dangerous nature of information and communications systems are imaginable. With the traditional network, the online threats emerged about when the wire, fibre and cable of the network were to be linked. At the moment, with wireless and mobile networks, the invisible threats are emerging in space where the electromagnetic wave of the network covers. Although the new technological outcomes are always accompanied by corresponding safeguards, historical instances have proved that the initial measures have usually been less effective. In addition, the legal framework is less ready and less prompt in reaction to the new phenomenon. As Clarke claimed that, with cybercrime (computer viruses), the collapse of banks, the launching of nuclear missiles, the shutdown of air traffic control, and the paralysis of the telephone network are all possible in the future (Clarke 1997, p. 227).

Conclusion

The Internet creates a space without a spatial or temporal boundary. Anyone with Internet access is connected to everyone else with Internet access in the world and is likely to be affected by the information that is published and the activities that are facilitated. All that not only provides chances for a social life, but also poses challenges to the social order. As a result, Gates (1995) stated that a significant aspect of the Internet is to get rid of remoteness, making it no difference between contacting a person in the next room and contacting another on another continent.

On the other hand, security and trust become essential to this new environment, which is constructed on systems vulnerable to attacks or abuse. Computers play different roles, such as means, media, target, tool, place, route in offences, and can be used in varied ways to prepare for other offences. People have already recognized that the unique character and the great value of the Internet for the user community is its decentralized structure (Rotenberg 1990, p. 16). What is tricky is that the maintenance of cyberspace order proves a challenge to the legal system. Many people are aware of the risks that people take when they go online. Quirchmayr (1997) pessimistically declared that the Internet became a paradise for all sorts of criminals (cited in Siponen 2001, p. 24). Interpol (2003) summarized the major threats as unauthorized access to and destruction of information in the processing, transporting, and storing stages. Information and communications technology poses enormous challenges to society, and clearly requires criminal-law reform.

Firstly, the objects requiring the protection of the criminal law have been expanded in the information age. The basic logic behind this is that, person, property and information are the three kinds of objects to be protected by criminal law, and that while both infringements of person and property are punishable offences, so should the abuse of information and communications systems punishable, too. Although criminal law has protected copyright, patent, trademark, and trade secret, the explicit literal provision for protecting "information" in criminal law is a development of the three recent decades. However, the provisions of different countries are not uniform. Disputes over changing the traditional criminal law are still taking place in some countries, and show the persistent resistance of the conventional notion. All these factors render the renovation of legislation an inefficient process. In order for criminal law to have actual effect, the sooner the renovation of the general theory and general part of criminal law are carried out, the better the criminal law can serve the information society.

Secondly, because of the expansion of the objects to be protected in the criminal law, it is very important to provide definition of new types of crimes, and to revise constituent elements of old crimes, in which information and communications systems become a new tool, object, place, medium, route, and means of traditional offences. This situation calls for the change of the special part of criminal law. If we say that the lag in the general theory of criminal law wastes resources in the legislation, the failure of the special part of the criminal law waste the resources in criminal justice, leaving a blank in deterrence as far as new types of crimes and new forms of old crimes are concerned. The effective implementation of domestic criminal laws increasingly depends on international coordination and cooperation, requiring realization to a far greater degree of the international consensus of substantial and procedural law.

Thirdly, the space of criminal justice is expanding beyond traditional society. The traditional crimes are fundamentally intra-national, trans-national, or at most international, while the new-fashioned cybercrimes are easily super-national and even virtual. That is to say, the crimes surpass the national power, while the super-national power in criminal justice has yet to be formed, being , restricted by the traditional principles of jurisdiction. In order to fill up the gap between the crimes and the power of criminal justice, international criminal law has formulated some new rules, though they are not widely accepted. A wider range of international action should be adopted in order to reduce the large expenses of time, money and human resources, and to decrease the further losses caused by crimes that are left unpunished in the process when there is this gap in criminal justice.

Fourthly, balance has not been reached between the influence of technology on criminal justice and on criminal phenomena, both of which are complex and involve positive and negative forces. The negative effect of technology on criminal justice and the positive effect on criminal phenomena point to a further failure of traditional criminal law: the inability of criminal justice and the inefficient deterrence against cybercrime increase the expected criminal benefits and lower the expected punishment. As a result, the increase of cybercrimes is inevitable. To resolve this problem, prompt enactment of domestic legislation worldwide and negotiation for international cooperation are required.

Fifthly, the dependence of criminal law on technology, and the interaction and mutual support between criminal law and technology should reach an unprecedented extent. Without the interaction of technology, criminal law could not obtain so great a deterrent effect. Similarly,

without criminal law, technology could hardly function solely in crime prevention. Both of them are necessary, but not sufficient. Although adding them up is not sufficient either, integrated countermeasures are of the utmost importance in cybercrime prevention.

In sum, the weak controllability of the Internet poses serious problems that fall into the domain of criminal law. There is a necessity for translating traditional law to cyberspace, translating domestic law in the international forum, and translating diversified provisions into a unified standard. Criminal-law reform is to put an end to the disorder of cyberspace where obligations and liabilities have not been sufficiently established and perpetrators of offences often run large.

However, we should also notice that the information society is not a new society but a new stage of the existing society, a social reality that is being re-expressed in the form of a re-encoding with a new coding system, as well as a new social order that is re-coping with the developmental tendency of society that has emerged in this new form. In the re-encoding process, the old codes remain or disappear, while the new codes emerge and grow. Cybercrime is one code in the re-encoding process of the information society.

REFERENCES

1. Bequai, A. 1978. *Computer Crime*, Lexington, Massachusetts, Toronto: Lexington Books.
2. Bequai, A. 1983. *How to Prevent Computer Crime: A Guide for Managers*. New York, Chicago, Brisbane, Toronto, Singapore: John Wiley and Sons.
3. Centre for Research in Electronic Commerce. 1999. *Measuring the Internet Economy*, The University of Texas at Austin.
4. Clarke, A. C. 1997. *3001: The Final Odyssey*, Hammersmith, London: Voyager.
5. Dodge, M. and Kitchin, R. 2001. *Mapping Cyberspace*, New York, New York: Routledge.
6. D'Ovidio, R., and Doyle, J. 2003. A Study on Cyberstalking: Understanding Investigative Hurdles, *The FBI Law Enforcement Bulletin*, volume 72, pp. 10-17.
7. Edwards, L. and Walde, C. (eds.). 1997. *Law and the Internet - Regulating Cyberspace*, Oxford: Hart Publishing.
8. Ekman, P. 1992. *Telling Lies: Clues to Deceit in the Marketplace, Politics, and Marriage*, New York: Norton.
9. Elliot, M. A. and Merrill, F. E. 1961. *Social Disorganization*, fourth edition, New York, Evanston, and London: Happer and Row Publishers.
10. Fisher, R. P. 1984. *Information System Security*, Prentice-Hall.
11. Forcier, R. D. and Descy, D. E. 2002. *The Computer as an Educational Tool*, third edition, Englewood Cliffs, New Jersey: Merrill-Prentice Hall.
12. Gates, B. 1995. *The Road Ahead*, New York: Viking.
13. GeoHive. 2006. Countries with Most Personal Computers. Retrieved 15 March 2016, from http://www.geohive.com/charts/charts.php?xml=ec_inet&xsl=ec_inet_top2
14. Gibson, W. 1984. *Neuromancer*, New York: Ace Books.
15. Grabosky, P. 2000. Cyber Crime and Information Warfare, The Transnational Crime Conference convened by the Australian Institute of Criminology in association with the Australian Federal Police and Australian Customs Service and held in Canberra, 9-10 March.

Retrieved 15 March 2016, from http://www.aic.gov.au/conferences/transnational/grabosky.pdf

16. Helmkamp, J., Ball, R., and Townsend, K. 1996. Proceedings of the Academic Workshop: "Definitional Dilemma: Can and Should There Be a Universal Definition of White-collar crime?" Morgantown, West Virginia: National White-collar crime Centre.
17. Howitt, D. 2002. *Forensic and Criminal Psychology*, Essex, England: Pearson.
18. Icove, D., and co-workers. 1995. *Computer Crime: A Crimefighter's Handbook*, O'Reilly and Associates.
19. Internet Crime Forum IRC Subgroup. 2001. *Chat Wise, Street Wise-Children and Internet Chat Services*.
20. Internet System Consortium (ISC). 2006. Internet Domain Survey. Retrieved 15 March 2016, from http://www.isc.org/index.pl?/ops/ds
21. Internetworldstats.com. 2007. Internet Usage Statistics-The Big Picture. Retrieved 27 July 2007, from http://www.internetworldstats.com/stats.htm.
22. Internetworldstats.com. 2015. Internet Usage Statistics-The Big Picture. Retrieved 15 February 2016, from http://www.internetworldstats.com/stats.htm.
23. Interpol. 2003. *IT security and Crime Prevention Methods: Explanations: A Report*. Retrieved 15 March 2016, from http://www.interpol.int/Public/TechnologyCrime/CrimePrev/ITSecurity.asp
24. Karygiannis, T., and Owens, L. 2002. *Wirelsss Network Security, 802.11, Bluetooth and Handheld Devices*, NIST Special Publication 800-48.
25. Kehoe, B. P. 1993. *Zen and the Art of the Internet*, Englewood Cliffs, New Jersey: PTR Prentice Hall.
26. Kelly, J. X. 2002. Cybercrime - High Tech Crime, JISC Legal Information Service - University of Strathclyde. Retrieved 15 March 2016, from http://www.jisc.ac.uk/legal/index.cfm?name=lis_cybercrime
27. Khosrow-Pour, M. 1998. *Effective Utilization and Management of Emerging Information Technologies*, Hershey: Idea Group Publishing.
28. Kingdon, J. 1994. Shooting the Messenger: The Liability of Internet Service Providers for Prohibited Expression. Retrieved 15 March 2016, from http://www.catalaw.com/logic/docs/jk-isps.htm
29. Kollock, P. and Smith, M. 1999. Communities in Cyberspace, in: M. Smith and P. Kollock (eds), *Communities in Cyberspace*, London: Routledge, pp. 3-28.
30. Levinson, D. (ed.). 2002. *Encyclopedia of Crime and Punishment*, Newbury Park, CA: Sage Publications.
31. Li, X. (2008). Cybercrime and Deterrence: Networking Legal Systems in the Networked Information Society. (Univerrsity of Turku). Turku, Finland: University of Turku.
32. Mowrer, E. R. 1942. *Disorganization: Personal and Social*, Chicago, Philadelphia, New York: J. B. Lippinatt Company.
33. OECD. 2004. *Second Organization for Economic Cooperation and Development Workshop on Spam: Report of the Workshop*, JT00174847, Busan, Korea, 8-9 September.
34. OECD. 2005. Task Force on Spam, Spam Issues in Developing Countries, DSTI/CP/ICCP/SPAM(2005)6/FINAL, Paris, France, 26 May 2005.

35. Pew Research Center. (2015). Social Networking Fact Sheet. Retrieved 15 February 2016, from http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet/
36. Quirchmayr, G. 1997. Selected Legal Issues Related to Internet User, *The Third International Conference on Reliability, Quality and Safety of Software Intensive System*, Athens, 29-30 May.
37. Robertson, S. 2000. The Digital City's Public Library: Support for Community Building and Knowledge Sharing, in Ishida, Toru and Isbister, Katherine eds. *Digital Cities: technologies, Experiences, and Future Perspectives*, Springer, pp. 246-260.
38. Rogers, L. R. 2001. *E-mail: A Postcard Written in Pencil*, Pittsburgh, PA: Carnegie Mellon University. Retrieved 15 March 2016, from http://www.cert.org/homeusers/email_postcard.html
39. Rotenberg, M. 1990. Prepared Testimony and Statement for the Record on Computer Virus Legislation, *Computer and Society*, volume 20, number 1, pp. 12-25.
40. Rowland, D. 1998. Cyberspace - A Contemporary Utopia? *The Journal of Information, Law and Technology*, volume 1998, number 3. Retrieved 15 March 2016, from http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1998_3/rowland/
41. Sadowsky, G., Dempsey, J. X., Greenberg, A., Mack, B.J., and Schwartz, A. 2003. *Information Technology Security Handbook*, Washington, DC: The International Bank for Reconstruction and Development.
42. Sikorski, R., and Peters, R. 1999. NET TIP: Digital Security, Part I, Science, 15 January, vol. 283. no. 5400, pp. 348 - 349, DOI: 10.1126/science.283.5400.348b.
43. Siponen, M. T. Five Dimensions of Information Security Awareness, *Computers and Society*, June 2001, pp. 24-29.
44. Summers, D. (director). 2003. *Longman Dictionary of Contemporary English*, Essex, England: Pearson Education Limited.
45. Syngress. 2002. *Scene of the Cybercrime: Computer Forensics Handbook*, Rockland, MA: Syngress Publishing.
46. Tehan, R. 6 February 2002. CRS Report for Congress, *Internet Statistics: Explanation and Sources*, Order Code RL31270.
47. UN. 2000. Crimes Related to Computer Networks: Background Paper for *the Workshop on Crimes Related to the Computer network, Tenth UN Congress on the Prevention of Crime and the Treatment of Offenders*, Vienna, 10-17 April. A/CONF. 187/10.
48. Wang, Y. 2001. *Hulian Fawang: Zhongguo Wangluo Falv Wenti* (Interlink Legal Web: Problem of Chinese Cyberlaw), Economic Management Press.
49. Wilbur. S. 1997. An Archaeology of Cyberspace: Virtuality, Community, Identity, in D. Porter, (ed.), *Internet Culture*, London: Routledge, pp. 5-22.
50. Zigrus, I. 2001. Our Virtual World: The Transformation of Work, Play, and Life via Technology, IGI Global, 2001.