International Journal of
Computer & Software Engineering

Commentary Open Access

Control of Knowledge and the Cyber Threat

Yair Sharan
Director FIRS2T, Jerusalem, Israel

Abstract

Cyber terrorism is one of the emerging threats in recent years. The research community and especially that related to cyber sciences can contribute to reduce the ability of people with malicious intent to realize their plans. Control of knowledge is one of the major measures in this direction. The aim of this commentary is to pay attention to this issue and to several ways in which control can be achieved without harming the important research in relevant fields.

Publication History:

Received: September 23, 2016
Accepted: February 04, 2017
Published: February 06, 2017

Keywords:

Cyber terrorism, Emerging technologies, Knowledge control, Code of conduct

Forward

Prof Leonard Kleinrock the Internet Pioneer from UCLA received the Dan David prize in May 2010 in Tel Aviv and stated that while developing the Internet he and his colleagues did not take into the account the possibility that in the future the Internet will be a tool for terrorists to realize their malicious intensions. They could have done more in the course of their research to minimize such a risk. It's of course not the only case in which the dark side of technology shows its ugly face. The Cyber field in general emerges to be one the sources for more threatening measures used by terrorists. Such kind of threats can unfortunately result in events with many casualties some caused by individuals mastering mass destruction technologies. The awareness to new threats due to new developing technologies is increasing and various studies are done to evaluate these potential threats and how to avoid them. One of these studies is the European FESTOS study focusing on emerging threats from future technologies. This commentary is mainly based on results of FESTOS study. Some of its results appeared in Foresight [1]. Later studies appeared which evaluated the threats and the ways to counter them [2]. Many scientists like Prof. Kleinrock are thus voluntary willing to apply measures which will reduce the accessibility of people with malicious intents to new knowledge and new technologies in order to prevent them from realizing their plans. One major measure in this direction is the control of knowledge.

Knowledge Control

The control of knowledge, the awareness of scientists and acceptance of codes of conduct are possible measures to treat the problematic issue of the dark side of technology in general and the risks emerging in cyber space in particular. All these measures try to approach the development of potentially dangerous knowledge on the level of the science community as a whole as well as the individual scientist who is involved in the development of new technologies or their applications.

Most mechanisms of knowledge control are seen in the academic communities as rather problematic. In several studies the complexity of the knowledge-control systems was investigated as well as relevant prevention measures applied. Aspects referred too were the state-of-the-art in the field of institutional control of sensitive knowledge and the state of the consciousness of these measures as well as the readiness to accept new mechanisms of controlling sensitive knowledge. The focus of such studies have been the necessary trade-offs between security, human rights and the freedom of research and knowledge creation.

Such evaluations yielded some conclusions that should be taken into account when designing advanced knowledge-control systems. Following are points to be considered:

1. The knowledge-control system should be based on "soft" control measures, including codes of conduct and internal mechanisms of knowledge control in different organisations (academia, research institutes and industry).
2. Bottom-up approach should be the main principle of knowledge-control systems, because governmental or international bodies are perceived as incapable of coping with all the threats resulting from different fields of 'sensitive knowledge'.
3. Education should play larger role in the knowledge-control system. Universities should add classes on threats posed by emerging technologies to the curricula in order to raise awareness of the students that will cope with 'sensitivity' of knowledge they will acquire or produce in future. 4. Moreover, some actions should be undertaken in order to raise awareness of risks emerging from new technologies and of existing control measures among the scientists. It may be done by connecting the funding of research with obligatory assessment of proposals evaluating if conducting such research may result in unwanted risks.
4. Last but not least, the preparedness to accept stronger control measures by the scientists and other 'sensitive knowledge' producers and users should be checked. Different research groups might perceive in different ways what the effect of control and prevention will be and how ready they would be to accept some new control mechanisms.

Based on the above insights and discussions on the effectiveness of knowledge control measures and their acceptance by the R & D community, a set of guidelines and principles for such a regime are formulated. This set assumes that researchers will be more willing to

***Corresponding Author:** Dr. Yair Sharan, Director FIRS2T, Jerusalem, Israely, E-mail: sharany@gmail.com

Citation: Sharan Y (2016) Advanced Clustering Method for Neurological Assessment Using Graph Models. Int J Comput Softw Eng 2: 109. doi: https://doi.org/10.15344/2456-4451/2017/111

accept measures of self control rather than imposed regulations. The bottom-up approach has already proven itself in similar issues such as the Helsinki accord on human experiments or the Hippocratic Oath in medicine. Regimes such as the control of Nuclear Weapons R&D show also that the research community is ready to comply with control regimes, once we deal with sensitive knowledge, in which case security gets priority. This bottom up approach might in some cases also result in regulations and even laws which are agreed in consensus between the law makers and the scientific community. This is further seen also when Bio-security is concerned. This paper assumes then that the Cyber community ,as well, will be ready to accept several regulations in order to reduce the risk of negative use of its research and breakthroughs..The latter will then realise the regimes agreed upon and contribute its share to increase the security awareness and level. Following are some principles that could be considered to realize such a regime of "soft" knowledge control:

Awareness, Consciousness and Education

Ongoing effort to raise awareness and understanding of the risks associated with the relevant field (e.g. Cyber) in general, and with dual-use scientific research in particular, should be maintained among the science community.

Oversight and Supervision Mechanisms

An efficient way to establish such a regime at relevant institutions is to upgrade and adapt existing safety oversight procedures. This is viewed as an optimal and practical solution for both R&D and service laboratories including those in the life and medical sciences. Local responsibility for the enforcement of security could be delegated to existing institutional safety committees in the academic sector.

Upgrade of Safety Regulations

Existing regulations on safety could be used in the short term as a model for institutional (e.g., university) procedures designed to prevent the seepage of potentially dangerous knowledge and information to potential criminal elements.

Oversight and Approval Of Publication Of Information Resulting From Dual-Use Research

This sensitive subject must be an essential part of a control policy. Given the potential risks involved, it is recommended to establish a system which will enable to oversee and approve dual-use research projects, as well as their results and publications by an internal mechanism based on the judgment of the academic community itself.

Consideration of Security Issues by Funding Agencies

Funding agencies as well as government research foundations (national and international research funds) will be able to require, as part of their approval process, security approval from the research institution in which the research will be conducted. This would ensure that these issues are considered by applicant institutions and that proper safety and security measures are enforced when needed. A similar policy is applied to day to ensure environment protection.

High Level Responsibility for Science Security

Science security should be dealt within the highest national level in the different countries involved. A national science security council could be established under the auspices of a relevant governmental ministry. It is important that such a body will have the necessary scientific knowledge as well a professional experience. This body will establish the science security regime and its enforcement mechanisms. This authority will thus have the national responsibility to maintain science security and take care for its sustainability. National authorities could then collaborate in international bodies thus enhancing security in the international level.

Conclusion

New research can attract malicious actors to potentially pose future risks to society. A policy should be conducted in order to try and reduce this threat. Avoiding accessibility of these actors to sensitive knowledge might be one of the dimensions of such a policy. Self control by the academic community might assure the success of such a policy. This major measure can be complemented by more measures which will help increase the awareness of the research community to the risks involved and will assist strengthening the cooperative attitude of scientists and researchers. These include targeted codes of conduct. Such codes remind members of a profession of their responsibilities in specific situations and can help create an environment in which ethical behaviour is the norm. A code can also serve as an educational tool and it can indicate to others that the profession is seriously concerned with sensitive issues and adopts principles of responsible innovation. Additionally special education courses can be tailored to teach students as well as more experienced researchers various ethical issues relevant to the problem concerned. The most important thing is to get researchers to think about the ethical choices and opportunities before they are faced with difficult situations in their professional practice. They might get then tools which will enable them to get educated decisions in cases of dilemmas and other sensitive situations.

Enhancing capabilities of researchers to confront these sensitive issues and raising their awareness to the need to take such considerations into their account might reduce potential threats while maintaining research and science without negative effects.

References

1. Hauptman A, Sharan Y (2013) Foresightof Evolving Security Threats Posed by Emerging Technologies", Foresight, October 2013.
2. Gordon T, Sharan Y, Florescu E (2015) Prospects for Lone Wolf and SIMAD terrorism, Technological Forecasting and Social Change. Volume 95: 234–251.