STUDY4CYBERWAR.COM

Critical briefing on attacks against Industrial Control Systems especially SCADA systems

Florian Grunert & Sebastian Kautz, MA

info@study4cyberwar.com
twitter.com/study4cyberwar

11/23/2010

Over the past few weeks Stuxnet created large amount of hype in the mainstream media. Some agents are exploiting this hype and filling newspapers and blogs with speculation. Of course the Stuxnet story involves different countries, cyberspace, infected power plants and Iran – who would not report about this? People are excited to hear how fiction becomes reality. This relatively short paper maps severe cyber-incidents from as early as 1985 onwards and adds some critical perspective to the mainstream hype around Stuxnet.

We are aware that speculations are the only investigative tool for the attribution problem in cyberspace. The attribution problem refers to the inability to trace an attacker, as the infrastructure of the internet gives the attacker a maximum degree of anonymity. This is an underlying problem in the field of cyber-security – every compromised machine is a part of this puzzle. In writing this paper, a second problem occurred - the problem of terminology. Researchers, security analysts and the media are using different terms for the same problems 1. As we intend to publish a quarterly journal, we shall definitively define terms in a special publication following this one. Any input, challenges and contributions are welcome!

Is this hype a sign that people, media, politicians, agencies and other elements of society aren't prepared for such incidents? We are asking “why“ because this kind of fear and overreaction is a result of an ill informed media and subsequently ill informed society.

Experts claim that this will be the beginning of cyberwar and an era of 'new threats' – although we do not have a precise definition of these threats, nor do we have an idea on how to attribute an attacker. There are some basic common ideas about cyberwar in the literature, but nothing more than a basic overview – *we simply have not had this happen before* and therefore we cannot know what the consequences will be. If one listens to expert opinions in the media, one realizes that they are talking about the same issues with different words. This has long been the great lingual problem known from other sciences and thus in itself is nothing new. In order to make a serious attempt to map cyber-events, we need to create a *spectrum* in order to set events into perspective with one another and to conventional threats.

This paper should not *relativise* the attack of Stuxnet, but we think that it should be analysed more rationally. This only works if people and the media can come to some understanding of the complex and dynamic interaction taking place between viruses, malware, other cyber issues and war, terrorism, crime and international politics.

We need an impulse in education about this new topic, otherwise we will end up being forced to seek advice from irrational speculators who will act out of fear and misunderstanding. This is already starting to happen in the media. There is a lot of speculation but this only indicates that we have to put more information online.

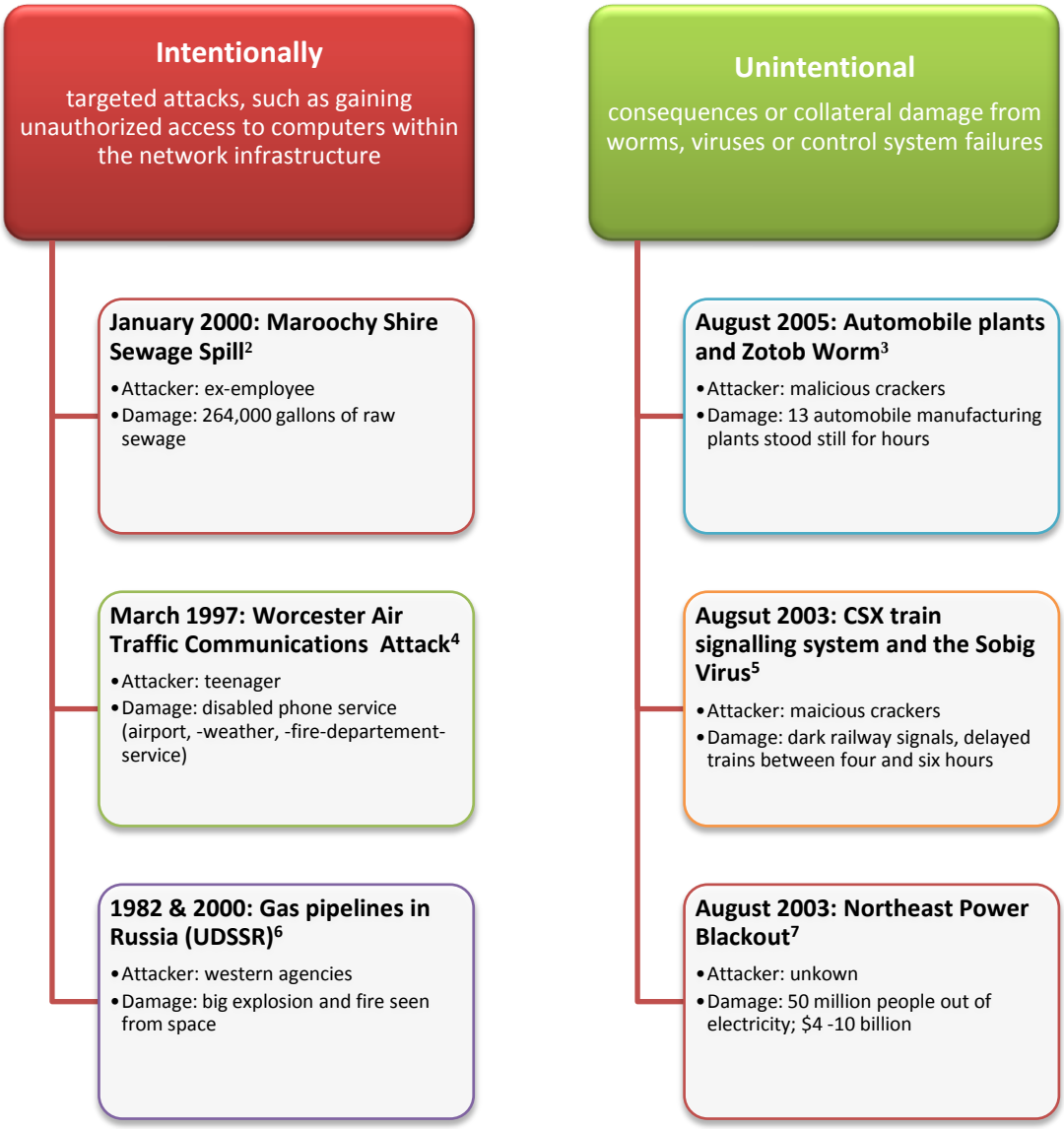
Feel free to inform yourself about cyberwar and the attribution problem. It seems only those who *cannot help* but inform themselves, are those who end up becoming informed. The media coverage of events thus far amounts to *mis*-information.

1 Hansen, L., Niessenbaum, H., Digital Disaster, Cyber Security, and the Copenhagen School, *International Studies Quarterly,* (2009) Vol. 53, pp.1156.

Stuxnet is a sophisticated attack but it was not the first of its kind on critical infrastructures to be running PLC or SCADA. A lot of researchers have published papers about SCADA/PLC/ICS problems and it has been known about for many years in security circles.

We will present a short list of attacks and incidents with SCADA systems which we took from this paper http://gspp.berkeley.edu/iths/Tsang_SCADA%20Attacks.pdf to show that similar events happened in recent decades. There is a lot of work to do, but it can be achieved with, good quality, concise, comprehensible and reliable information - and not with the hype and scaremongering of uninformed experts.

Table 1



2 http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/
3 http://www.industryweek.com/articles/hacking_the_industrial_network_18937.aspx?Page=1?ShowAll=1
4 http://edition.cnn.com/TECH/9703/18/cyberwars/index.html
5 http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=13100807
6 http://en.wikipedia.org/wiki/Siberian_pipeline_sabotage
7 http://en.wikipedia.org/wiki/Northeast_Blackout_of_2003

The above table shows attacks on critical systems that would today be classified as cyber-attacks in the domain of cyberwar. However, the increasing number of incidents over the past 25 years and the undisclosed amounts of losses in the industry lead to a politicisation of the cyber-security issue. And rightly so. It is the state's responsibility to protect its citizens and industries, but there is no need to overestimate this threat in relation to what has happened in the past and what is possible in the future. *Genocide could not take place because of a malicious cracker for example.*

In order to illustrate the problem of *response* further, we would like to draw a comparison to some different global hype situations and the resulting 'wars' and 'campaigns', and their respective achievements.

The 'war on terror' is a widely and wildly debated issue that has dominated global security policy over the past decade. Terrorism, especially against the US was present well before, but it took the spark of 9/11 to take security to a new level. If previous attacks had been taken more seriously, then the decisions taken post 9/11 may have not been as rushed and driven by fear.
The second example is the politicisation of climate change and the 'global response' to the subject. Climate change is a particularly interesting issue, as the nature of the threat is different to what politicians and international theorists got used to over the centuries. It is a non military, non state threat – climate change is the direct result of human industrialisation and the resulting change of the chemical composition in the atmosphere – it really is the sum of all fears.
Honourable scientists like James Lovelock and Rachel Carson knew this as early as 1962 and 1975 respectively, and published great works in order for the problem to be recognized. Although their publications, and the grass roots green movement lie far in the past, it was only in 2009 that the world leaders met at the Copenhagen Climate Summit to start negotiating a *global* strategy to what is a global problem. The meetings were largely confusing and clouded by power struggles, especially with regards to the emerging powers like Brazil, India and notably, China.

The climate change issue and cyberwar have a lot of common features, as they threaten a large part of the world population, yet, these threats do not *seem* to be imminent. This might be the reason that governments hesitated for so long - to at least seem to try to make progress on the climate change issue. Cyberwar on the other hand threatens the military, economic and political stability of nations and that is why governments are forced to act. But security is expensive and CEOs do not want to spend money. It is necessary that governments are able to build a framework in law which leads to more protection of critical infrastructures.

Over the last two or three years it has become apparent that the governments of the most powerful and biggest nations are preparing to cover terrain in the 5th dimension of war, namely cyberspace, and this *must* then become a matter of concern for international theorists and lawyers.

Stuxnet, in our view, is only another signpost along the way towards a new internet. Net- neutrality and security may give rise to new forms of regulation and policing of the internet. It was the purpose of this article to show that any response, be it unilateral, bilateral or international, has to be thought through and must be made in accordance with *users*.
The failure of the international community to find decent approaches to the “war on terror”, the

“war on drugs” and the slow response to climate change, sheds a bad light on the outcome of any attempt to regulate the internet. This claim can even go further, as the lack of international cooperation can be blamed for the patchiness of international law and law enforcement. The problems humanity faces today are not confined within a nation or a continent – they are global in every respect.

We would like to encourage you, private person, academic or decision maker to engage in a long term debate here on study4cyberwar before making hasty choices. We trust and believe in Open Source and would like you to join our community.

The *study4cyberwar* team has compiled a number of resources related exclusively to the StuxNet issue. Please feel free to visit our website.

http://study4cyberwar.com/news.html Search with Ctrl+F „STUXNET” and you will find a lot of links to reports, pages, interviews, papers and blogs.

Feel free to contact us for more information! Please send us notes, advice and new stuff you can not already find on *www.study4cyberwar.com*

- End of Paper -