On Contamination in Information Ecosystems

A Security Model Applied on Small and Medium Sized Enterprises

Bengt Carlsson & Andreas Jacobsson

School of Engineering

Blekinge Institute of Technology, PO Box 520, S-372 25 Ronneby, SWEDEN

{bengt.carlsson;andreas.jacobsson}@bth.se

Abstract¹

On the Internet, digitally active small and medium sized enterprises (SME) face numerous security risks. When SMEs join networks, business ideas and malicious activities may interfuse. E-mail marketing, remote control and information gathering are replaced by spam, virulent programs and spyware. In this paper, we use the concepts of information ecosystems to describe a security model where, as a background, humans are presumed to act as Machiavellian beings, i.e., behaving selfishly. Based on this notion, we analyse behaviours initiated by network contaminants and their effects to an entire ecosystem. The contribution of this paper is the security model, which permits a comprehensive view on the risk environment in virtual networks (like the digital SME community).

1. Introduction

On the public Internet, there are numerous insufficiencies, vulnerabilities and threats that in accumulation make it a very risky environment to conduct business operations in [1][14][24]. Even so, the European Union (EU), with support from organisations representing small and medium sized enterprises (SME), advocates that SMEs should adopt into digitalisation, i.e., connect their businesses to the public Internet [9]. But, the rising occurrence of network contamination or malicious software (malware), e.g., virulent programs, spyware and unsolicited commercial e-mail messages (spam), pose a great risk for the success of the intended SME digitalisation. This paper attempts to capture the current risk domain for SMEs by introducing a new security model inspired through theories of evolution-

ary biotic ecosystems. The security model, here applied on the digital SME community, illustrates a comprehensive view of risks, countermeasures and consequences to an entire system or society. Even though the security model is applied on the European SME scenario, it may also be applicable to other communities or networks.

This paper is organised as follows. First, we begin with the background presenting the current state of SME operations in Europe. In 3, we give three examples of common malware problems that occur on the Internet, and that in combination, add to the increasing network contamination. Then, we discuss the analogy of the SME community as an evolving information ecosystem. In 5, we present the conceptual view of the security model, and in 6, we apply it on the SME scenario. Then, we discuss the model, its application and possible effects on the SME community. In the end, conclusions are presented.

2. The SME Community

The SMEs within Europe represent a vast majority of the enterprises and are the main source for developing new products and services [11]. Within the EU, there are 20 million SMEs, of which most hold less than ten employees per company [13]. In comparison, there are 40.000 large enterprises with more than 250 employees in the entire Europe.

As a new strategic goal, the Lisbon summit² manifested that, by year 2010, the EU should be the most competitive and dynamic knowledge-based economy in the world [10]. In order to reach such a goal, it is clear that it is within the sector of SMEs that the joint efforts must be put. The key to growth is through digitalisation of business concepts and processes [13]. In this context, Information Communications Technology (ICT) inno-

1. This work is part of the EDEn project, Enterprises in the Digital Economy, European Cluster for Innovation within the 6th Framework Programme for research and technology development within the European Union.

2. A two-day economic summit with senior ministers from all EU-member countries that was held in Lisbon, Portugal, on March 23rd-24th, 2000.

ventions are imperative enablers for technological progress and economic expansion. ICT innovations bring new markets, re-organised and increased value chains, and the manufacturing of novel services and products.

The wanted effects of digitalising SMEs are increased efficiency and productivity [9]. Then, SMEs abilities to expand value-chains, develop new products, services and markets also grow. With the adoption to digitalisation, experts predict other advantages to the SMEs, such as, e.g., sharing customers, expertise, markets, and costs [9][13]. Minimising disturbance costs and risks, yet maximising the value of resources and processes are, in this view, imperatives for any SME.

As it seems, only fragments of the SME sector have adopted or plan to adopt to the digital economy [26]. The reasons for rejecting digitalisation are both numerous and diverse (e.g., depending on core business operations, language barriers, IT-resistance and business culture) [20]. However, in reality, most SMEs lack digital alternatives that consider standardised and cost-efficient digital business processes that are usable to the everyday activities [9]. According to the EU, one important factor in this setting is the enforcement of IT-security [26].

IT security is an area of strategic, operative and systemic importance to any SME aiming for digitalisation. In principle, all information on the public Internet can be made publicly available. In turn, this raises questions of business confidentiality, integrity, availability, intelligence and corporate privacy. In this setting, there is therefore a great need for knowledge as well as useful and cost-efficient pragmatic solutions [26].

Today, most of the SMEs that are digitalised are not primarily distributing digital products and services, but use the public Internet as means for conducting business activities (e.g., marketing, customer communication, etc.) [12]. Due to its nature, the public Internet contains numerous threats, weaknesses and insufficiencies that in accumulation make it a very risky environment for companies to conduct their businesses in. So, the public Internet is not really the best place to go when wanting to digitalise businesses. Assuredly, it is really the only setting with high availability and low adoption costs, yet fit for customer marketing and communication. The digital SME community wants to be able to participate on the public Internet, and at the same time they want reliable and secure systems for business operations [12].

3. Network Contamination

Large virtual networks (like the Internet) may be exposed to negative feedback [2][23], or as we prefer to call it; *network contamination*³, which bring about significant risks and severe consequences to all of the network

participants. In example, hidden malware may employ a network and its range for distribution purposes, and selfish actors may abuse the network for the spreading of spam.

In effect, there is a distinction between the two major categories of unwanted, or unsolicited malware. In the first category there are pure malware programs, i.e., those that are distributed solely with a malicious and/or destructive purpose. In this category, we typically find virulent programs, worms and Trojans. Normally, this category poses threats to security, capacity and stability of systems and networks. In the second category, we find such malware that is only partly distributed with a malicious intent, but mainly with a commercially-driven purpose. Typically, this software category includes, e.g., spam messages, spyware, adware, and browser helper objects. Even though these sorts of commercially-driven software usually also impose threats to system and network security, capacity and stability, their main cost is that they invade the privacy of the users.

A distinction such as between the malware categories may be helpful when analysing the risk domain for Internet users (such as digital SMEs) in order to implement security measures. For an SME, the consequences of being exposed to purely malicious software may be loss or tampering of data and system resources, unnecessary costs for network and system maintenance. Exposure to commercially-driven malware may be loss of sensitive corporate information, breaches in copy-right, unnecessary costs for network and system overload, and privacy protection. However, as we shall see later on, pure malware can be used in business strategies, and commercially-driven malware can be used for purely malicious actions.

Of course, the occurrence of any kind of malware is not beneficial when building a secure and stable digital SME economy. However, risk is the cost for doing business, so it is really not possible to eliminate all malware risks. Instead, knowledge and awareness must be gained so that the risks could be managed to an acceptable SME level.

In summary, ensuring security for SMEs participating in virtual networks is critically important if the positive effects of adopting into new technologies are to arise. But the security domain facing digital SMEs is not easily understandable, therefore we attempt to capture the security challenges at hand by using the complexity of a wide-ranging information ecosystem as an analogy.

3. The word "contamination" is used by anti-virus companies in order to describe malware programs causing unwanted and negative effects to networks and computers. We use the concept in conformity with this view, that is to describe when certain software pollute or litter information ecosystems.

4. SMEs and Information Ecosystems

One way to model the digital SME community is to regard it as an emerging information ecosystem similar to a biotic ecosystem. The structure of such an ecosystem is basically determined by interactions between actors and the environment, and by interactions between different actors. An ecosystem is able to adapt to changing conditions, can easily scale up or down, and has an openness and universality. The process that shapes the patterns of actors within an ecosystem is called natural selection [28]. The human mind may be examined using a Darwinian explanation [7][15], which we further on will describe as a Machiavellian intelligence. Successfulness for the single participant rather than loyalty towards the system will be favoured, i.e., we should expect selfish, vigilant behaviours among actors. Cooperation, belonging to a business group and so on, must hold some advantage for the actor compared to being alone.

Like an information ecosystem, the digital SME environment has an openness and can quite easily scale either up or down with the adoption of new technologies. Also, the fact that SMEs act in a commercial setting, where economic climate shapes the patterns of the actors, makes it resemble the process of natural selection within an ecosystem.

The inhabitants in a digital surrounding are the services and products acting on behalf of the companies and of the humans. In this analogy, digitalised SMEs take part in a global ecosystem, the Internet that consists of suppliers and customers, acting as malicious and selfish actors. For the local SME, this means that, besides conducting ordinary business activities with companies and customers, it has to take the “misbehaving” of other actors into consideration. Expressed in terms of natural selection, cooperation must hold some degree of advantage compared to acting alone for the enterprises, because self-interest is universally and essentially favoured [4][5][29].

Today, script-kiddies, crackers, criminals and possibly also rival competitors form the “malicious and selfish society”. On the Internet, the number of successful attacks has increased, and the amount of computers and servers breached by intrusions have augmented [14]. Specifically, this means an accentuation of risks for SMEs, and for SME services and products. In conclusion, the actors and inhabitants of the ecosystem are at risk.

As will be further examined in 5, trust (which is a necessary component in any relationship, physical or digital) is more problematic to ensure in a growing virtual network. Therefore, the security of an SME business partner becomes a prioritised concern. Because, even though good intentions and trust may be in place between SMEs, an SME cannot always trust its partners. A virus may use a

Figure 1. The Security Model

partner’s e-mail address list to distribute itself to the contacts on that list, and thus infect the customers and business partners of that SME. If so, there will be problems recognising a trusted sender from a distributor of virus or malware. The insecure settings of a business partner will therefore cause security problems to all parties in the environment. The increasing occurrence of new malware technologies distributed by malicious and selfish actors make the elements of risk both apparent and urgent.

5. A Security Model within an Information Ecosystem

To describe the dynamics within an information ecosystem, a security model is outlined in Figure 1. In summary, the model describes how selfish actors take part in an escalating competition and/or enhanced exploitation over resources that result in settled conflicts, chaotic ecosystem breakdown or in the implementation of legislative solutions. In the model, we use and discuss the concepts of Machiavellian beings, arms race, the tragedy of the commons and the red queen hypothesis.

Instead of further examining the desires and intentions of the actors, we analyse the selfish environment within the ecosystem. Of course, actors may be separated into trusty users versus malicious attackers, or malicious behaviours into business strategies versus intrusion attempts, but the comprehensive dynamics are more easily seen without this restriction.

The basic setting in the security model is constituted by actors equipped with *Machiavellian intelligence*, i.e., bringing out self-interest at the expense of others [8]. We must consider the dynamics caused by such selfish behaviours, and a totally friendly digital surrounding should therefore never be expected. SMEs are managed by humans, and humans are, as a result of the evolution, competitive and selfish actors. In this sense, the neighbours of a Machiavellian being are also behaving selfishly. In contrast to the physical world, it is more convenient to abuse a vir-

tual network in order to commit crimes and frauds on the Internet, due to, e.g., anonymity, technical superstructure and lack of limited physical distance.

The consequences of behaviours within a selfish surrounding may either be an escalating competition or an enhanced exploitation over accessible resources within the ecosystem. According to biological ecosystems, we introduce arms race or the tragedy of the commons for these activities respectively.

The skills of the actors are refined through an evolutionary competition called an *arms race* [3][21]. An arms race between actors, either humans or digital inhabitants, or between groups of actors signifies that the (antagonistic) activities made by one group are retorted by countermeasures by another group, which in turn makes the first group react, and so on. This property may act as a self-adjusting quality set to improve an information ecosystem over time. On the Internet, there are numerous examples of arms races, which we will come back to in 6.

If common resources (e.g., bandwidth, e-mail media) are misused by a selfish actor, a *tragedy of the commons* [16] situation may occur. The tragedy of the commons describes an event where the costs caused by the actions of a selfish individual are shared by all participants, while the selfish individual gets all benefits from these actions. In such a competitive surrounding, there is an obvious risk that the majority of the individuals will get worse off. Thus, a common solution should in the long run favour everyone, because the alternative is a breakdown.

The resulting stage of an enhanced resource exploitation may be “*the red queen hypothesis*” [21][27]. This expression stems from what the red queen said to Alice (in Wonderland): “here, you see, it takes all the running you can do to keep in the same place”. In effect, the red queen hypothesis means that each business must evolve as fast as it can merely in order to survive. The red queen hypothesis is represented by three possible outcomes, namely settled conflicts, chaotic ecosystem breakdown or the implementation of legislative solutions. In Figure 1, the arrows indicate plausible connections between behaviours and results. A dashed arrow indicates a metalevel solution to the problem, i.e., a solution derived from parameters outside the model.

From a biotic ecosystem’s point of view, arms race normally means a settled conflict where each actor or group of actors find a suboptimal solution, i.e., arms race tends to act in the background. In other words, a refined balance between antagonists restrain the actors from misusing the system.

On the Internet, a company or a service that is not evolving with the same pace as its competitors is being outmanoeuvred by market progress, i.e., the breakdown of a tragedy of the commons or an arms race situation occur. The same is true if commercially-motivated or purely mali-

cious actors exploit resources as a consequence of the tragedy of the common situation.

In the security model, distributed solutions like “informed actors” or “free market forces” would not essentially improve the utility of the ecosystem. Such solutions are based upon the (contradictory) selfish actors or the activities already mentioned above. Instead, legislative solutions, where demands are initiated, are needed. Although, such a solution is strictly speaking outside the model since it is not regulated as a natural consequence of the activities within the ecosystem. Instead, legislative solutions are regulated by fabricated (as opposed to natural) authorities. In addition, the success of such a metalevel solution is hard to foresee without knowing all the details of the legislative alternatives.

6. The Security Model Applied on SMEs

In this section, we explore three examples of network contamination where malicious activities are realised by selfish actors that abuse a virtual network (such as the public Internet) for their own good. Two of the examples (spam and spyware) belong to the commercially-driven software category, whereas the third example (virulent programs) represent purely malicious software. However, even though purely malicious software usually is not designed with a commercial intent, we have seen that pure malware also can be used in order to complete a commercial plan. Albeit a virus generally is designed to create chaos in a system, that chaos may very well be an important ingredient in a commercial strategy initiated by a rival competitor.

So, in this setting, one common property for the three examples is that neither one of them are solely designed and distributed for malicious purposes only, instead they are parts of comprehensive business strategies represented by billion-dollar industries. Here, we use the theory of information ecosystem and the security model to analyse these phenomenons (see Figure 1).

6.1. Spam and the Distribution of Advertisements

During late 2003, the total spam rate reached 50 percent of all e-mail messages that traversed the Internet [14]. Calculations indicate that on the average, each spam needs 4.4 seconds for handling, i.e., reading and deletion. With the distribution of 20 billion spam messages per day, an astronomical, accumulated 25 million hours are needed for the handling of spam. According to reports, a single spammer may hold up to 200 million e-mail addresses, to which transmission is conducted with a very limited extension of means. So, a vast distribution of spam may be performed by only a small number of spam-senders.

Spam distribution, or as some marketers prefer to call it; e-mail marketing, is an important ingredient in many marketing strategies. To SMEs, sound e-mail marketing (in contrast to bulk spam distribution) could be a highly cost-efficient method for conveying offers that could allow an SME to reach a substantially large amount of potential customers. But today's mass e-mailing is littering the Internet and thus contributing in the adding of network contamination.

6.1.1. Machiavellian Spammers. Currently, spam messages are mainly distributed as parts of comprehensive business strategies (i.e., with selfish purposes). A few network participants use the availability of an entire network for their own good, with no regards to whom that must carry the consequences. Due to that spammers primarily take themselves into consideration, spammers are behaving as Machiavellian beings.

6.1.2. Spam and Arms Race. Spam may invade computers as a result of an arms race. Spam-filters and lists of blocked accounts and servers may reduce the amount of spam, but spammers hiding their intended message and the occurrence of more effective data-harvesting methods may instead increase the rate of spam. Arms races force anti-spam measures to evolve as a result of spam activities, which in turn make the spammers react, and so on. In this light, as users, SMEs probably accept false positives, but true negatives are unacceptable, i.e., they do not take the risk of throwing away an important message even though the vast majority of e-mail messages are spam.

6.1.3. The Tragedy of the Commons. As a result of the red queen hypothesis, spam messages do not pay their own costs [18]. This is a tragedy of the commons situation where a single spammer may violate the use of bandwidth, storing capacity or in the end the whole virtual network. As long as the costs for spam activities are shared among the entire network, there are no real incentives for a spammer to stop.

6.1.4. The Red Queen Hypothesis. There is a risk that computer applications may become inapplicable as a result of heavy spam messaging activity. According to the red-queen hypothesis, an application under attack must evolve as fast as it can merely to survive. If the proportion of spam messages exceeds a critical limit, users may find it inconvenient to use e-mail systems over the Internet. Most spam messages are automatically generated, but removing them is done manually (if we do not dare to rely on spam filters). Human capacity is the same today as yesterday, so a hundredfold or a thousandfold expansion of spam traffic may render in that the whole e-mail application collapses, i.e., as chaotic breakdown in the security model. For SMEs, this

would mean that sound e-mail marketing is be nothing but an elegant economic theory. Settled conflicts would also be a potential solution, but if such a scenario is to be effectuated the very source of spamming must be removed, i.e., the economic incentives for spamming must be eliminated. As the Internet is constructed, this is not a plausible outcome. One solution that, to some extent, has been effectuated so far is the implementation of legal impediments [6], but observations indicate that these initiatives are not powerful enough to set aside spamming [18].

6.2. Virulent Programs with Business Intentions

During the summer of 2003, Sobig.f infected 200 million e-mail messages across the Internet during its first week of activity. Estimates indicate that Sobig.f impacted 15% of large corporations, and 30% of SME organisations. Sobig.f was the biggest/virulent virus over the last four years [1]. Due to that Sobig.f also fit the properties of a worm, it infected the host computer when an enclosed file was opened by the user. Inside the computer, Sobig.f used addresses from the local address book for further spreading [1]. As part of the payload, harmful software was downloaded and installed on the infected computer, which also permitted further installations of new malware and reconnections of network traffic. The original idea behind Sobig.f was to install a spam proxy-server on the targeted desktop in order to use the infected computers as distribution nodes over the Internet [1]. However, this step was not completed because of that too much attention drawn made it impossible for the virus to operate secretly in the background. In this context, Sobig.f is an example of how purely malicious malware may be used as a part of a business strategy.

In general, a virus has no utility to an SME (in opposite to what might be the case with spam), and therefore it can only be considered a cost for belonging to the network. Even so, virulent programs are more common than ever and they, in accumulation, seriously contribute to network contamination.

6.2.1. The Machiavellian Virus Makers. In the digital environment, there are Machiavellian humans acting not only as traditional hackers, but also as cunning businessmen. As the Sobig.f example shows, a virus may consist of, not only the distribution mechanism and the payload process, but also of a comprehensive business idea (the installation of spam proxy-servers). Like spam, virulent programs are typically developed and spread for selfish purposes.

6.2.2. Virus and Arms Race. The ongoing arms race facilitates a reaction within hours from anti-virus companies. So, if, for instance, an SME has invested in qualified secu-

city software, a regularly upgraded anti-virus protection should solve the immediate and realised threats. However, history has shown that for every successful anti-virus protection, there is a new successful virus, and so on.

6.2.3. The Tragedy of the Commons. A distributor of virus uses the network for spreading virulent programs with little regards to the infected parties. The usual model for a virus is to infect as many nodes on the network as possible in the least conceivable amount of time. Even though some attacks may be directed to targeted parties, infections typically strike others as well. Also, arms race indicates that every virus is retorted by countermeasures taken by the anti-virus organisations. Either way, it is the gullible network participants and the network service providers that carry the costs of virus (and of anti-virus protections).

6.2.4. The Red Queen Hypothesis. The behaviour of virtual network neighbours are essential for local security settings, i.e., even an excellent local security policy may fail in a surrounding of insecure settings. In the Sobig.f example, e-mail addresses were distributed from infected hosts, and a heavy network overload influenced all nodes on the network. For both anti-virus protection and for virus programs, they must continue to evolve in order to stay on the same place, i.e., as long as there is no great disadvantage for the anti-virus protection, the conflicts will be more or less settled. Although, a serious increase of virus distribution may render in that an entire digital SME community may end up in chaotic breakdown. Also, some examples of the implementation of legislative solutions exist in the U.S. today, however, due to the global structure of the Internet such initiatives are inevitably fruitless.

6.3. Spyware and the Collection of Business Information

A “mistake” made by the creators of Sobig.f was its too successful spreading mechanism. If the purpose was to install a spam proxy-server on the local computer, a much slower distribution would have been preferable. A spyware without any attention from the anti-virus community, but with full access to local computers would have been the perfect tool. Reasonably, the main intention for Sobig.f was not to damage the host, but to use it as a leverage point in order to reach more extensive parts of the Internet.

A spyware is a program that covertly gathers user information through the user’s Internet connection without the user’s knowledge of it [19]. Typically, spyware programs are bundled with ad-supported free software [22], such as file-sharing tools, instant messaging clients, etc. Once installed, the spyware monitors, e.g., user activity on the Internet and transmits that information in the background

to third parties [25], such as advertising companies. Spyware usually also includes some adware components, i.e., software set to display advertisements and offers to the user (adware), browser helper objects and cookies. Also, some spyware programs act as Trojan horses allowing installation of further malware. One of the major American ISPs set to measure the occurrence of spyware on the computers connected to their network. They discovered that the total number of spyware instances was 27.8 per scanned computer [24]. The number of Trojans and system monitors approached 18% respectively, whereas the instances of adware were five for each scanned computer. Also, experts suggest that spyware infect up to 90% of all Internet-connected computers.

Potentially, a spyware could have some value in terms of allocating usable customer information to an SME. Even so, a spyware program normally creates problems such as that it normally imposes threats to security and privacy, and also degrades system and network capacity [22].

6.3.1. The Machiavellian Spyware Intruder. Typically, a legal grey area is exploited by the spyware actors, since they in most program licenses actually specify that information may be gathered for corporate purposes. However, the usual model is to collect more information than have been asked for [17]. Here, the only focus is to maximise the value of the spyware distributor, rendering in selfish behaviour.

6.3.2. Spyware and Arms Race. Spyware is usually problematic to detect and remove from infected host computers since users install the carriers of spyware, e.g., file-sharing tools, on a voluntary basis (typically, the file-sharing tool cannot run if the spyware is removed). Then, the message distribution part is taken care of by the spyware servers connected to the file-sharing network. This could mean that spyware programs can operate like a slowly moving virus without the distribution mechanisms usually otherwise included, and without the detection mechanisms visible for anti-virus programs. Today, some anti-spyware tools exist, which generally are useful for locating spyware, however, the removal of located spyware is difficult (even for an anti-spyware tool) since it normally is interfused with, e.g., the actual file-sharing program. But, it seems that the anti-virus community has begun to react on spyware. In combination with anti-spyware tools they may become an effective measure in the struggle against spyware. However, the history of virus versus anti-virus has shown that such an effort will be retorted with newer and more advanced spyware programs, and so on.

6.3.3. The Tragedy of the Commons. Today, it can be hard to distinguish a spyware program from a virus. Even though a virus typically is designed for destructive pur-

poses, such properties can also be added to a spyware. Given this, security is more and more difficult to uphold. Even though some anti-virus tools are designed to react on spyware programs, most such applications still do not regard a spyware as a virus. In the SME setting, an unsuccessful spyware is stopped by anti-virus/anti-spyware applications, whereas successful spyware programs continue to gather and transmit sensitive information to third parties (e.g., competitors) over the Internet. In example, by letting SMEs and their employees use commercially supported freeware, such as file-sharing tools, an SME faces the risk of being monitored by potential competitors or malicious actors that selfishly use network nodes for their own good. The consequences, e.g., in terms of bandwidth overconsumption, are left to the network.

6.3.4. The Red Queen Hypothesis. In contrast to a virus, spyware programs may operate in the background in such a relatively low speed that they are deceptively difficult to detect and remove. In combination with that spyware may include components set to cause destruction in a system, the consequences may be just as dire as with a regular virus. Although, settled conflicts may really be a reasonable solution to the spyware problem, it may just as well lead to chaotic breakdown. Increased amounts of spyware programs will lead to overconsumption of system and network capacity rendering in unnecessary costs for maintenance, etc. In the end, it is the network nodes that must share the costs. In effect, a chaotic breakdown may be the ultimate result. Since spyware programs are a relatively new phenomenon, there are no imperative legal restrictions to comment on. Albeit, should such one be found, it is reasonable that it will face the same kind of problems as spam and virus legislation.

7. Discussion

Business ideas and malicious activities may sometimes interfuse when SMEs join networks. E-mail marketing, remote control and information gathering are replaced by spam, virulent programs and spyware. The different examples above converge to a more general Machiavellian business idea. Spyware enables for the spreading of e-mail addresses that may result in the receiving of spam or in the gathering of critical business information. A virus may install a spam proxy-server on an unprotected computer. All together, an SME should be very careful about storing confidential data. In many SME cases, information commodities are more important than production capacity. Examples of this could be that stolen information may be used to increase efficiency and productivity in a competitor's production processes, or that deletion or tampering with critically important data may be devastating in terms of loss of internal values for SMEs.

Selfish actors participating in an arms race force SMEs to exclude security issues from business activities. The occurrence of malware means that even though an SME computer may be secure, a breached computer owned by a network neighbour can cause harm to the SME. So, the security of a neighbour very much becomes every network user's concern. No single SME facing the problems of, e.g., spam messages and/or malware programs are capable of solving the difficulties single-handed. Instead, security threats are foremost a joint problem to larger communities, such as the EU. This is also illustrated through the security model.

To an SME, the internal security is important, but not sufficient. Selfish actors solve problems by introducing an arms race, and they may also cause a tragedy of the commons situation. The successfulness of an SME network depends primarily on the cooperation between the actors. So, cooperation must hold advantages compared to acting alone. Because of that SMEs take part in a dynamic and complex ecosystem, security issues should be separated from other business activities within the digital economy.

We could easily extend each of the network contamination examples to include other results from the red queen hypothesis. However, just as biotic ecosystems, the future is not predictable because of too many unexpected circumstances. The security model includes necessary but insufficient information for anticipating the future. Humans have the possibility to act on inappropriate behaviours by restricting the positive outcome of such an activity through legislative solutions. This is not the same as stopping the selfish behaviours of Machiavellian actors. The arms race and the tragedy of the commons will just take another less harmful direction. Hopefully, with the development of a digital economy for the SMEs will benefit from such a security model.

8. Conclusions

There are two principle ideas in this paper. First, there is the security model, which permits an overall perspective on the risk environment that face large virtual networks. Second, there is the discussion concerning the three forms of network contaminants (included in the model).

On the Internet, digital SMEs face numerous security risks. When SMEs join virtual networks (such as the Internet), business ideas and malicious activities may interfuse. Spam messages, virulent programs and spyware are three examples on that. We use the concepts of information ecosystems to describe a security model where, as a background, humans are presumed to act as Machiavellian beings, i.e., behaving selfishly. The process of such an act is an ecosystem conducting an arms race where selfish actors perform a tragedy of the commons situation that

results in chaotic breakdown, settled conflicts and/or the implementation of legislative solutions. We use the information ecosystem and the security model to analyse distribution of advertisements, virulent programs with business intentions and collection of business information. One conclusion from applying the security model to the digital SME scenario was that the risks facing SMEs is a joint problem. It cannot be faced by SMEs one by one. Instead the entire SME community and all of its interested parties (e.g., the EU) must join together and form a digital environment where risk are minimised and utility is maximised. Here, our contribution is a description of risk environment facing digital SMEs.

References

- [1] Arce, I., "More Bang for the Bug - an Account of 2003's Attack Trends", *Security & Privacy*, vol. 2, no. 1, pp. 66-68, 2004.
- [2] Choi, S-Y., Stahl, D.O., and Winston, A.B., "*The Economics of Electronic Commerce*", Macmillan Technical Publishing, Indianapolis IN, 1997.
- [3] Dawkins, R., "*The Extended Phenotype*", W. H. Freeman and Company, Oxford UK, 1982.
- [4] Dawkins, R., "*The Selfish Gene*", 2nd ed., Oxford University Press, Oxford UK, 1989.
- [5] Dennett, D.C., "*Darwin's Dangerous Idea*", Allen Lane Penguin Press, London UK, 1995.
- [6] Directive 2002/58/EC of the European Parliament and of the council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 2002., http://europa.eu.int/comm/internal_market/privacy/law_en.htm, 2004-06-10.
- [7] Donald, M., "*Origins of the Modern Mind*", Harvard University Press, London UK, 1991.
- [8] Dunbar, R., "*Grooming, Gossip and the Evolution of Language*", Harvard University Press, Boston MA, 1997.
- [9] "E-Business Analysis and Benchmarking", commissioned by the European Commission, 2004., <http://europa.eu.int/comm/enterprise/ict/policy/econ-anal/index.htm>, 2004-06-10.
- [10] "E-Commerce and the Internet in European Businesses (2002), Report on the Results of the ICT Usage of Enterprises 2002", Eurostat, commissioned by the European Commission, February 2002., <http://europa.eu.int/comm/enterprise/ict/studies/entr-ict-2002.pdf>, 2004-06-10.
- [11] European Association of Craft Small and Medium Sized Enterprises, <http://www.ueapme.org/EN/index.shtml>, 2004-06-10.
- [12] "The European E-Business Report" (2003 edition), commissioned by the European Commission, July 2003., <http://www.ebusiness-watch.org/marketwatch/resources/E-Business-2003.pdf>, 2004-06-10.
- [13] The European Office of Crafts, Trades and SMEs for Standardisation, <http://www.normapme.com/English/ict-en.htm>, 2004-06-10.
- [14] Ferris Research, <http://www.ferris.com/>, 2004-06-10.
- [15] Gärdenfors, P., "*How Homo Became Sapiens: On the Evolution of Thinking*", Oxford University Press, Oxford UK, 2003.
- [16] Hardin, G., "The Tragedy of the Commons", *Science* vol. 162, pp. 1243-1248, 1968.
- [17] Jacobsson, A., Boldt, M., and Carlsson, B., "Privacy-Invasive Software in File-Sharing Tools", in *Proceedings of the 19th IFIP International Information Security Conference*, Toulouse France, 2004.
- [18] Jacobsson, A., and Carlsson, B. "Privacy and Spam: Empirical Studies of Unsolicited Commercial e-Mail" in *Proceedings of IFIP Summer School on Risks & Challenges of the Network Society*, Karlstad Sweden, 2004.
- [19] McCardle, M., "How Spyware Fits into Defence in Depth", SANS Reading Room, SANS Institute, 2003., <http://www.sans.org/rr/papers/index.php?id=905>, 2004-06-10.
- [20] "Management Training in SMEs", commissioned by the Organisation for Economic Co-Operation and Development (OECD), OECD Publications, Paris France, 2002.
- [21] Maynard Smith, J., "*Evolution and the Theory of Games*", Cambridge University Press, Cambridge MA, 1982.
- [22] Sariou, S., Gribble, S.D., and Levy, H.M., "Measurement and Analysis of Spyware in a University Environment", in *Proceedings of the ACM/USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, San Francisco CA, 2004.
- [23] Shapiro, C., and Varian, H., "*Information Rules*", Harvard Business School Press, Boston MA, 1999.
- [24] Spyaudit, <http://www.earthlink.net/spyaudit/press/>, 2004-06-10.
- [25] Townsend, K., "Spyware, Adware, and Peer-to-Peer Networks: The Hidden Threat to Corporate Security" (technical white paper), PestPatrol, 2003., <http://www.pestpatrol.com/Whitepapers/PDFs/SpywareAdwareP2P.pdf>, 2004-06-10.
- [26] "UEAPME's Annual Report 2002", UEAPME, Brussels Belgium, 2003., http://www.ueapme.org/docs/general_pubs/jaarvl2002.pdf, 2004-06-10.
- [27] van Valen, L., "A New Evolutionary Law", *Evolutionary Theory* 1, pp. 1-30, 1973.
- [28] Williams, G.C., "*Adaptation and Natural Selection*", Princeton University Press, Princeton NJ, 1966.
- [29] Wilson, E.O., "*Sociobiology - The Abridged Edition*", Belknap Press, Cambridge MA, 1980.