

David Bénichou · Serge Lefranc

## Introduction to Network Self-defense: technical and judicial issues

Received: 1 February 2005 / Accepted: 9 May 2005 / Published online: 29 October 2005  
© Springer-Verlag 2005

**Abstract** This article aims at presenting the main issues resulting from self-defense protocols implemented to defeat any launched network attack. The authors, namely a network security expert and an examining magistrate, built a universal model and submitted it to a variety of typical cases in order to anticipate the main consequences of usual self-defense reactions. The above-mentioned cases range from the most stupid attack to the most sophisticated one. Consequences are expected to occur on both technical and judicial levels. The possibility that a battle may be won on a technical level could have disastrous effects on a judicial level. What we usually call “self-defense” applies both to blind attacks and targeted assaults (which may use viral codes). Judicial issues will be set forth according to a general scheme which is common to main criminal law systems (mainly French and American ones).

**Keywords** Legal issues · Network self defense · Retaliation · Response intrusion

### 1 Introduction

Our article is based on a public presentation made by the authors during a conference organized by the French Armament Agency Infowar Center (CELAR) in November 2003. The objective was to confront the technical and legal aspects of the network self-defense. At that time, no particular research, especially bibliographic research, was done.

While writing this article, we discovered a wide corpus of literature about network self-defense, often called active

defense. Almost all these publications focus on the subject’s technical part, often without mention of the legal aspect, or with vague mention suggesting that the legal problem was a solved parameter (Aggressive Network Self-Defense 2005): “*Legal consequences are known: the model assumes that all legal consequences are known*” [chapter 9, pp. 269]

We did not base our work on what was previously done but noticed that our approach is converging and want to underline that any purely technical approach is dangerous, because it only deals with half the situation; the American military approach of the topic seems to share this point (Information Operations ).

Hence, for an informed public, our article may appear not to represent the state of the art of active defense. We will not discuss the latest algorithms or concepts. We will show that actions which permit victory on the technical level could be disastrous on the judicial level, and so, therefore active defense is not a so good idea as people would like to believe.

Indeed, to undertake any self-defense reaction, one has to identify the attacker. In physical life, it is easy because we are often face-to-face with the attacker. In cyberspace, the situation is complicated because the methods of identifying the attacker are not trustworthy. It is easy for an attacker to falsify his identity, and thus, not enable us to fight back. One study bypasses that crucial point (Information Operations , pp. 52) “*The initial discussion assumes correctly knowledge of the computer attacker’s identity and confidence in the US ability to characterize his intent.*”. In real life, such assumptions are often unfulfilled, and thus all the strategy is built on sand. We will also show, that eventually, this type of system could lead to a massive denial of service attack that would spread like a virus, following a chain reaction.

Pro-self retaliation commentators insist naturally on the technical efficiency of active defense, as they are not experts in law. It is easy to draw a simple yet inaccurate comparison between real world and cyberspace. Any public speech on that subject, from people working in official administration could be interpreted as an encouragement for those who will equip themselves with self-active defense systems and those

D. Bénichou (✉)  
Juge d’instruction, Cour d’appel de Paris, Pôle financier, Paris, France  
E-mail: david.benichou@justice.fr

S. Lefranc  
Centre d’Electronique de l’Armement,  
Ministère de la défense, Rennes, France  
E-mail: serge.lefranc@dga.defense.gouv.fr

who market these systems. But the story does not tell who will pay the lawyers, nor the diplomatic bill.

## 2 Legal aspects

The origins of the of self-defense justification are hard to find, as they seem to have always existed. According to Ciceron, self-defense was a rule which has no age “*non scripta sed nata lex*”. The Roman twelve table’s law made the distinction between day and night assaults, which we can still find in our modern states. The Jewish “law of retaliation” (*lex talionis*) was probably one of the first attempts to introduce the principle of proportionality in the defense act, in that way it was a smoother law (you will not request more than you lost, for fair remedy).

In most civilized states self-defense justification provides, under certain circumstances, judicial immunity or excuse when using force to reply to an attack. Our purpose is to focus on the main legal conditions of self-defense, in order to uphold the universality of our model. Each judicial system has its own particularities, but most of them share the same definition of what we call self-defense. To illustrate this point, we will point out the conditions of self-defense in various countries. The common definition of self-defense will be integrated to build a valuable model, to improve, in a second time, the judicial and technical consequences.

It is important, from a judicial point of view not to restrain the study to the law of the country where the defender is located, but also anticipate what could be the consequences in the attacker’s country, or in some intermediate state. As we will see, the self-defense justification is based on three main conditions whatever the judicial system is: the reality of the attack, the immediate response whose purpose is to thwart the attack (i.e. excluding revenge) and the proportionality principle.

### 2.1 France

#### 2.1.1 Self-defense principles

In France the self-defense justification is defined by the law, in the penal code wherein article 122-5 distinguishes between the defense of a person, and that of property.

Art. 122-5 ([www.legifrance.gouv.fr](http://www.legifrance.gouv.fr)): *A person is not criminally liable if, confronted with an unjustified attack upon himself or upon another, he performs at that moment an action compelled by the necessity of self-defense or the defense of another person, except where the means of defense used are not proportionate to the seriousness of the offence.*

*A person is not criminally liable if, to interrupt the commission of a felony or a misdemeanour against property, he performs an act of defense other than wilful murder, where the act is strictly necessary for the intended objective, the means used are proportionate to the gravity of the offence.*

We can draw a table that shows the differences between the two situations, Defense of a person and property (Table 7).

**Table 1** Different situations in french self defense

Defense of a person	Defense of property
Commanded by necessity	Strictly necessary
Burden of disproportion’s proof to the prosecution	Defender will have to prove that the defense was proportionate (lethal defense is not possible)

So, when one defends an IT system, what does one protect? — a property or a person? Even if an IT system remains an entanglement of cables, computers, and data, it cannot be classified under the “property” column. Even if some IT professionals are very sentimentally attached to their computer, it cannot be considered to be a “person”. But we can assert that an IT system is more than just a “property” and is sometimes vital for persons. An IT system provides some functions that can’t be reduced to simple property. In a hospital, the IT system can regulate patients lives. A satellite can play a major role in transmitting communications between people. There is a sort of scrolling line where defense has to be fixed. This line starts at the “the property defense” and ends at “person’s defense”, from the lowest, to the maximum value to protect. For the defender, the judicial location of the IT system on this line would be a key element. According to our analysis, there is an opportunity to create a specific rule for vital IT systems, that would require the most extensive defense capabilities, even lethal, when lives are under threat.

The French penal code article 122-6 is quite peculiar when replaced in an IT context: *a person is presumed to have acted in a state of self-defense if he performs an action to repulse at night an entry into an inhabited place committed by breaking in, violence or deception; to defend himself against the perpetrators of theft or plunder carried out with violence.* So, in cyberspace — when is it night? When is it day? Is your server room an inhabited place? Are personal data the inhabitants of your server? Beyond these provocative questions, we can summarize the main conditions of qualified self-defense under French law:

1. **A real offence.** The defense act should respond to a real and illegal offense (self-defense against force used by state authorities wouldn’t be allowed, unless the authorities have completely out-stepped their prerogatives). The attack could be aimed against the defender himself, against someone else, or against a property. If the attack aims at property, conditions are stretched: the defense should be absolutely necessary and scaled to the gravity of the attack, the means must be proportional to the gravity of the offense (homicide, in that case is always forbidden).
2. **A simultaneous response.** The defense should be simultaneous to the attack (a “postattack” defense is a retaliation, retaliation doesn’t grant any justification, in such a case, the defender becomes the attacker and exposes himself to judicial pursuits).
3. **A proportionate response.** The defense should be strictly proportional and reasonable with regard to the attack’s gravity.

### 2.1.2 The soldier's exception

The recent 2005-270 French law of March 24, 2005 defining the general statute of the soldiers introduces a significant extension of self-defense justification for the soldiers:

Art. 17: *I - In addition to the cases of self-defense, the soldier is not penally responsible when deploying, after warnings, the armed force absolutely necessary to prevent or stop any intrusion in a highly significant zone of defense and to carry out the arrest of the author of this intrusion.*

*Constitute a highly significant zone of defense, the zone defined by the Minister for the defense inside which are established or stationed military goods whose loss or destruction would be likely to cause very serious damage to the population, or would endanger the vital interests of national defense.*

*A Council of State decree lays down the methods of application of the preceding subparagraphs. It determines the conditions under which are defined the highly significant zones of defense, conditions of delivery of the authorizations to penetrate there and procedures of their protection. It specifies the methods of the warnings to which the soldier proceeds.*

In theory an IT system could be part of a “highly significant zone of defense”; in, that the IT network is part of the organization behind the protected perimeter. Therefore, there is no reason why cyber-soldiers wouldn't be authorized to respond by armed force (active defense systems?), after appropriate “warnings” (warning packets?). The question of the application of this extension to an IT perimeter is not clearly stated. The penal law should be strictly interpreted (lenity principle); therefore, if this text doesn't clearly rule that this exception also applies to a military network, it would probably be considered as irrelevant by a court or a prosecutor.

## 2.2 United States

### 2.2.1 The self-defense principles in American criminal law

<sup>1</sup>The self-defense in the United States is mainly a creation of the common law. No federal legislation expressly defines what is self-defense but in several criminal cases, courts apply common law defenses where applicable. In many states, the legislature has adopted criminal laws which give exemption from criminal liability, although it is limited to the use of physical force. In New Jersey the NJSA 2C-3-4(a), states that: “[...] *The use of force upon or toward another person is justifiable when the actor reasonably believes that such force is immediately necessary for the purpose of protecting himself against the unlawful force by such other person on the present occasion.*”. Federal common laws and state statutes often treat defense of others and defense of property similarly. The extent to which these defenses can be applied to IT attack scenarios remains even unclear.

The model penal code (MPC), which is only a project held by the American Law Institute, gives a definition of

self-defense justification that is compliant with the three main conditions seen before (Model Penal Code ). However, defense of others and defense of property seem to be both applicable (Karnow 2004–2005), as an IT attack is never directly targeted against a human being.

According to Dressler (1995), self-defense has three elements: “it should be noted at the outset that the defense of self-defense, as is the case with other justification defenses, contains: (1) a “necessity” component; (2) a “proportionality” requirement; and (3) a reasonable-belief rule that overlays the defense”.

18 U.S.C. 1030(f) also has an explicit exception for certain kinds of government actions: “*any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States*”<sup>2</sup>.

### 2.2.2 The issue of retreat

The question of the duty to retreat was raised by the common law of homicide and extended to other forms of defense by the MPC. When the defender has the ability to retreat, the defense response is no longer necessary, thus the self-defense justification will fall. The American courts are divided on that point: 28 states adopted the duty to retreat rule against 21 which consider that the defender benefits to the “right to stand one's ground” and two lets the jury decide. (District of Columbia and Texas).

In an IT context, the duty to retreat does mean that the administration should at first consider whether he can or not disconnect the system to escape from the attack. This capability could be automated: if the system notices a typical attack, such as a flooding, or a worm-spread, we could imagine a rule that moves the system on the network, in order to protect it by a safety retreat (eg., modification of IP addresses, in order to allow outgoing communication but not incoming traffic).

## 2.3 Israël

The Israeli law of self-defense<sup>3</sup> states that it is possible to protect oneself, someone or property, even by a lethal response but only if the attack was not preceded by a provocation.

The conditions are similar to French or American systems: defense has to be immediate and proportionate and, directed against an unlawful attack. Moreover, the Israeli law states that the unlawful offense could be aimed not only the life but also the liberty of the defender. That's an original point, and it could be interpreted as a broader definition of self defense, but quite hard to appreciate in an IT context.

<sup>2</sup> Thanks to Kenneth Harris, USA liaison magistrate, Paris

<sup>3</sup> Israeli Self-Defense law “Haganah etsmite” 39 from 1994, penal code, chapter V “justification defenses”, 2, art. 34/10. Thanks to the information service, Israel Embassy in Paris.

<sup>1</sup> Thanks to the Center for Computer Assisted Legal Instruction, Mineapolis, [www.cali.org](http://www.cali.org); Norman Garland's lessons on Self-Defense, and Duty to retreat

## 2.4 Russia

The article 137, Chapter 8 of the Russian penal defines self-defense in four points:<sup>4</sup>

1. The fact of causing damage to a person who attacked you, does not constitute a crime, in the event of situation of self-defense, i.e., to defend yourself, your rights or other people, the interests of the community or the State defined by the law, or from a socially dangerous attack, if this attack was made with violence, danger to the life of the defendant or another person or then with the immediate threat of such a violence.
2. Protection against a person attacking without violence, danger to life or immediate threat of such a violence is legal, if the defense is made without excess regarding the limits of self-defense such as acts which do not obviously correspond to the gravity of the attack.
3. Do not exceed the limits of self-defense, the acts made by the defendant, if this one, because of the unexpected character of the attack, could not objectively evaluate the degree of danger of the attack (law of the 14.03 2002 and 8.12.2003).
4. The right of self-defense belongs equally to everyone, whatever one's profession or position. This right belongs to everyone independent of the possibility of avoiding the social danger of request for assistance from another person or an official service of the state.

*Italy* In its article 52, the Italian penal code adopts the same definition, based on the three main conditions: “*Non è punibile chi ha commesso il fatto per esservi stato costretto dalla necessità di difendere un diritto proprio od altrui contro il pericolo attuale di una offesa ingiusta, sempre che la difesa sia proporzionata all’offesa.*”.

## 2.5 Kingdom of Morocco

In Kingdom of Morocco, the “dahir” N° 1-59-413 of 26 November 1962<sup>5</sup>, adopting the penal code is very similar to the French penal code. In Chapter V “justification defenses” art. 124, the Morocco penal code, defines the self-defense as a necessity to defend oneself or somebody or a property with a defense proportionate to the gravity of the attack. The article 125, adopts the two same presumptions that are in French law (attack by night or theft committed with violence).

## 2.6 The issue of the continuing attack

In all legal systems, the act of defense must be contiguous to the attack. Before its preemptive attack, after its payback or retaliation. When the attack is continuing in time, we think

<sup>4</sup> Thanks to Agnes LALARDRIE, French liaison magistrate, Moscow

<sup>5</sup> Thanks to Houda HAMIANI, office of the liaison magistrate, France Embassy, Marrakech.

that the retreat duty should be preferred, than self-defense that should be initiated only when necessary (when official defense forces are not able to act rapidly). If the defender has more time to prepare an attack, it means that he also has more time to protect his network or to call for assistance. Therefore the self-defense would not be so spontaneous as it should be. One of the justifications for the self-defense is that this act is instinctive, not prepared. The law is stricter when the defender has plenty of time (continuing attack) to plan a response that would be more a retaliation than an act of necessity. What should be borne in mind is that you should always prefer the retreat (protection of the system), the alert of authorities, and as a last resort – the defense answer.

## 3 Our model: the ARS

### 3.1 Origin of our model

What is a model, what can it do, what can't it do and why make models? Basically, a model is a simplification of the world. We isolate a class of phenomenon and try to explain it by using rules and hypothesis.

As a simplification, each model has its own limits and field of validity. It is essential that the user of a model be aware of its field of validity and remain critical with respect to the results. If it is not the case, it opens the door for all kind of abuses. A model is not reality: apart from its limits, the results do not represent the reality, they just represent the property of the model.

One cannot affirm that a model is true or false. A model is a tool which provides results more or less accurate, depending on the hypothesis and conditions of use. A good model must be predictive, i.e., it must make it possible to predict, in a certain way, the results of an experiment. This predictability can be qualitative or quantitative according to whether the model can predict behavior or can predict the value of measurable data.

Based on these assumptions, we designed our model of network self-defense. The purpose of the model was to be as simple as possible in order to make very few hypothesis and assumptions. It is possible to elaborate a complicated model but it will then require more hypothesis, and will therefore not be broad enough. We decided to take the opposite path: by analyzing the facts, we tried to reduce the hypotheses to a minimum. By doing so, we pretended to have a model that is able to deal with basic and complex situations, but essentially be as general as possible.

### 3.2 Hypothesis of our model

The hypothesis we made took into consideration two different aspects: the legal and technical approach.

The hypothesis we made is in accordance to what was previously presented in the legal context (at least in France!): a

self defense action must have some basic characteristics: it must be an immediate response and be adequate to the intensity or the nature of the attack detected.

On the technical side, the hypothesis must take into account what kind of threat we can encounter on a network, more specifically, what is the nature of network threat a computer can undergo? Basically, they are of two kinds: the intrusion type and the denial of service type. The first one concerns the integrity and confidentiality of the data, while the second one concerns their availability. Both of them can be identified easily based on the first packets captured on the network.

We are not going to detail the mechanism of attacks, it is already well documented. In case of both the intrusion and the denial of service type attacks, we can use a database of previous attacks and their characteristics, detect the network packets corresponding to them. Detection is important and, without a good database, we can miss the detection. Similarly, if the attack is not present in the database, its characteristics are unknown, and thus, we cannot detect it.

The detection of denial of service is straightforward if one uses the correct attack database. The detection of an intrusion is more complex, but there is an assumption we can make to simplify this situation. An intrusion is often preceded by a fingerprint scan. It allows the attacker to gain information about the ports and services which are open, and also the nature of the operating system used (see NMAP ([www.insecure.org](http://www.insecure.org))). It is a necessary phase of information for a successful attack. In other words, if we can detect a fingerprint scan, there is a great probability that an attack will follow shortly. In order to be as accurate as possible, we must also make a distinction between a soft and a massive fingerprint scan. An attacker can just try to probe the port 80 with a SYN packet, or try to probe each of the 65,535 ports by sending different kinds of malformed packet (like NMAP is able to do). There are two kinds of item that can be detected: a non-intrusive fingerprint scan and an attack packet or intrusive fingerprint scan (an analogy exists in the non-computer world: there is a difference between an intruder that knocks on the door and checks the backdoor, and an intruder that breaks the door or tries to force it open; it is the same with fingerprint scan).

So, the hypothesis of our model is as follows: upon the detection of a fingerprint scan or an attack packet, the system will automatically answer according to the nature of what is detected. The answer will be immediate and linked to the intensity or the nature of the attack detected (if the attack is a simple SYN packet to the closed port 80, there is no good reason for the system to answer by a massive denial of service). The attack packet category represents a massive fingerprint scan, a denial of service or anything else that will be more intrusive than a basic fingerprint scan.

### 3.3 Characteristics of the model

Our digital model is called the automated response system (ARS). It takes two levels of threat in input and three levels of response in output. The threats are defined and categorized

**Table 2** Principle of action and reaction in legal perspective

Hostile events	Counter measures	Legal qualifications (French, Art. 323-1 and follow from the code penal)
Fingerprint	Store and process data	/
Attack packet	Denial of service	Fraudulent access (data modifications)
Attack		

under hostile events (Table 2). The answer will depend based on the nature of the hostile event.

For example, if we detect a fingerprint scan, we can answer with Counter measure 1 (Store and process data). If we detect an attack packet, we can answer by a denial of service Attack, depending on the nature of the elements detected.

### 3.4 A basic implementation of the ARS

The implementation of this model is straightforward with tools that already exist. It does not need a lot of special development but instead linking applications.

In order to detect an attack, we are going to use a network sniffer in correlation with a database of known attacks and their characteristics. Each time a dangerous packet transits the network, the system will detect it.

In order to answer to the attack, we are going to implement basic tools that allow the execution of the countermeasures previously defined: store and process data, generation of a denial of service or realization of an attack.

So the ARS system (Fig. 1) is composed of three modules: a monitor system that captures packets on the network, are attack database which allows the comparison between the packets captured and the one corresponding to an attack, and the answer system which responds to an attack packet.

## 4 Using the ARS . . .

We just explained how the ARS was designed. Now, we are going to use it and describe what happened on the computer that runs the ARS system. After doing so, we analyze, and not just describe, the situation in order to see if what happened is the result of only one situation, or if multiple causes exist that lead to the reaction of the ARS system.

The situation is as follows: a computer with the ARS system is used in order to protect the company, ARS Inc. There are no assumptions made and all the data gathered by the ARS system are based on the one provided by the packets received.

The ARS system monitors all packet that comes to ARS Inc. It detects a packet coming from address IP A that match a denial of service attack from the attack database. As it corresponds to a denial of service attack, the ARS system decides to answer to address IP A by a denial of service. This address

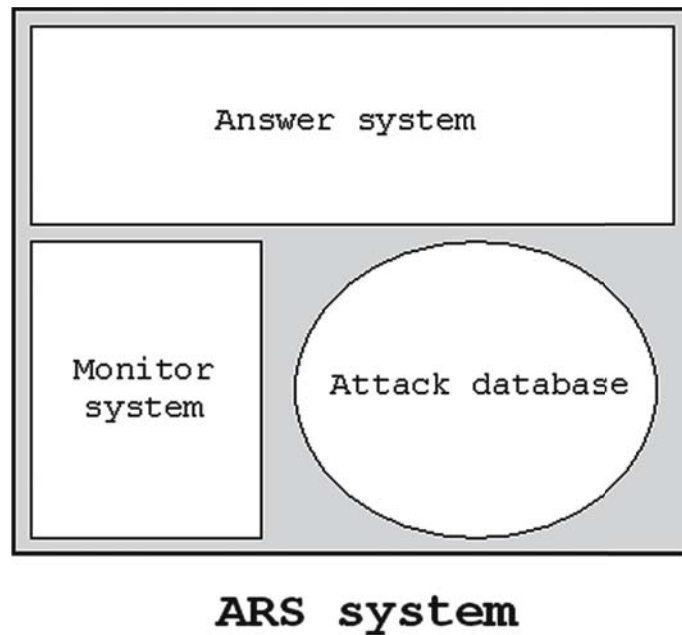


Fig. 1 Architecture of the ARS system

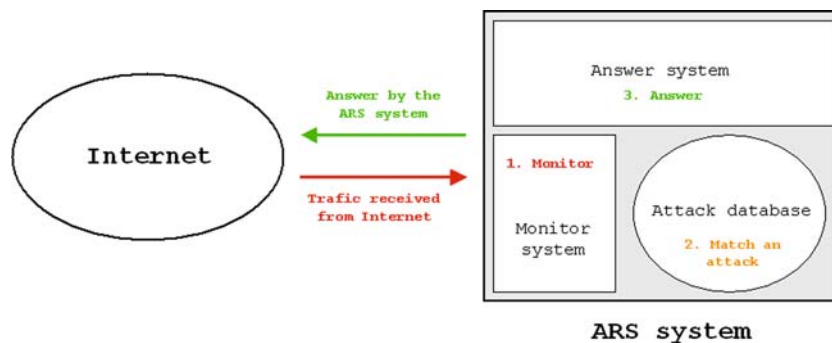


Fig. 2 The ARS system in action

is the one present in the IP header of the packet corresponding to the denial of service.

#### 4.1 Scenario 1: the Kamikaze attack (stupid attack)

The attacker launches the attack from his computer, so the address detected by the ARS system is the correct one and the self-defense mechanism works perfectly. We call this attack the “stupid” attack because no serious attacker will ever use his own machine to act.

In this case, the ARS system plays its role, correctly identifies the attacker and answers back in accordance with the mechanisms of self-defense.

#### 4.2 Scenario 2: the careful attack

The ARS system in the careful attack is shown in Fig. 2. Here, attacker launches an attack from a computer he compromises (computer B). The ARS system will identify computer B as the source of the attack.

In this case, the ARS system detects an attack from computer B and launches a countermeasure. The computer B effectively launched the attack, but it was not the actual source of origin: it was actually conducted by the attacker on computer A. Computer B was merely used as a bounce machine. Thus, the ARS system failed to correctly identify the origin of the attack. From the point of view of computer B, ARS Inc is an attacker since it has launched the countermeasure against it.

#### 4.3 Scenario 3: The smart attack, the “lightning packet”

The ARS system in the smart attack is shown in Fig. 3. Here attacker launches the attack from its computer but it spoofs the address IP of a computer which uses an ARS system. The ARS system of ARS Inc will identify computer C as the origin of the attack, and as computer C also uses an ARS system, its ARS system will identify an attack coming from ARS Inc.

In this case, the ARS system detects an attack from computer C. This computer is not the source of the attack but ARS



Fig. 3 The ARS system in the kamikaze attack

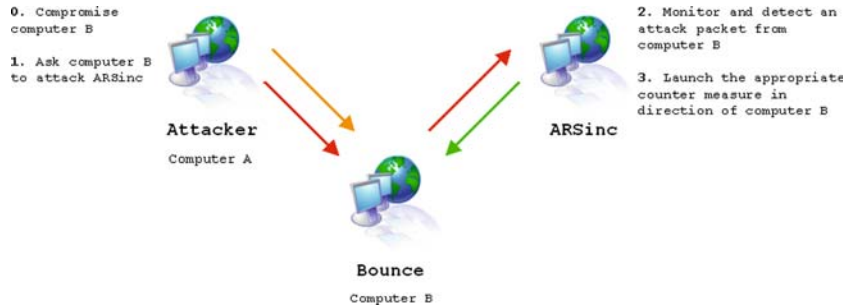


Fig. 4 The ARS system in the careful attack

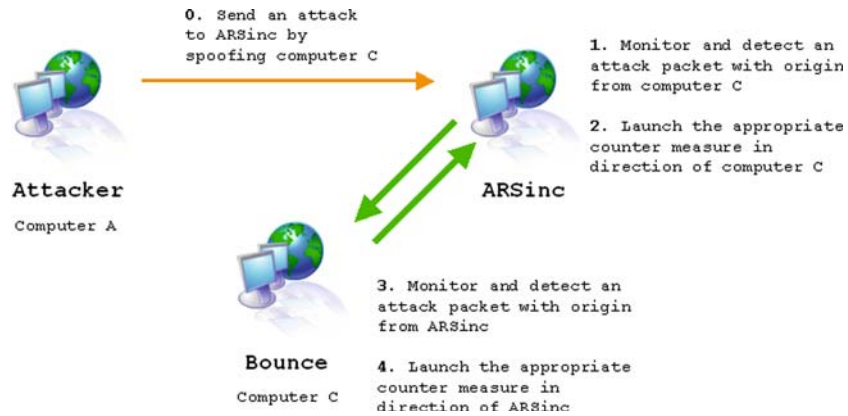


Fig. 5 The ARS system in the smart attack

Inc still launches a countermeasure against it. As computer C is also equipped with an ARS system, the countermeasure launched by ARS Inc is detected as an attack; so the ARS system of computer C answers by a countermeasure against ARS Inc. ARS Inc detects the computer C countermeasure as an attack and answers by another countermeasure, which is going to be detected as an attack by computer C. Quickly, the two computers are going to make a massive denial of service against each other.

What is interesting about such an attack is that the real offender has to only send one packet, the “lighting packet”, which will initiate mutual aggression between the victim (initial target) and the spoofed IP machine (secondary target). Now imagine that our offender is very smart. When choosing the secondary target, he will probably choose a network that will enhance the credibility of the attack, and cause serious diplomatic complications. In such a case, let’s assume that state A and B embassies have ARS systems. The C state

would only send one packet spoofing the IP of B (secondary target) to A (primary target), and then let A and B mutually attack (defend) their networks. It’s a double gain for the attacker: on the technical level he would have probably managed to cause damage to the A and B networks, and at less denial of service; on another level, he would have created a legal and diplomatic crisis between A and B.

#### 4.4 Consequences when the ARS system is present on multiple system: the chain reaction

In the case of a smart attack, we saw that it is easy for an attacker to make two systems unavailable if they use an ARS system to protect themselves.

This last scenario could lead us to an effect well-known in the virus community: the quick spread of a virus. In our case, we are not facing a virus or a worm, but the effect could

**Table 3** Risks and gains of the use of an ARS system

Type of attack	Risk encountered by the defender	Gains
kamikaze (stupid)	No judicial risk except if the answer was not proportioned	1 (Attacker defeated)
kamikaze (stupid) careful	Response aimed at a wrong target High risks to be sued by the wrong target	-10 (Attacker missed and Judicial issues)
Smart (lightning packet)	Response aimed at a wrong target with an escalation process The wrong target was a sensitive organization belonging to an ally eventually Diplomatic situation Scandal	- 100 (Attacker missed, Diplomatic issues)

be very similar in the case of multiple companies using an ARS system to protect themselves.

The contamination will grow as quickly as the number of systems implementing the ARS system and becoming victims of an IP spoof.

Our model is not only a proof of concept. There already exists this type of mechanism on the Internet. An illustration is given by the domain snert.com (Ossir mailing list): When you send an e-mail to this domain, the SMTP server answered the following comments (at least in April 2005):

Despite the fact that this is not legal (in France at least), imagine what can happen if the SMTP server that send an e-mail to snert.com implements the same kind of mechanism? There is no doubt that it can result in the detection of an attack and thus lead to an answer by the system will further result in the same situation as the one mentioned in scenario 3.

## 5 Conclusion

At the present time, it is difficult, even impossible, to identify the source of an attack with certainty. It is easy for an attacker to modify the source of an attack, or to launch it from a compromise computer. In both cases, there are no possibilities to be sure of the origin of the attack.

So it is not possible for an ARS system (or any network self-defense equipment) to surely identify an attacker, and thus, answer by a countermeasure mechanism. The only possible reaction that is both technically and legally possible is to send an RST packet to a packet detected as an attack. It will shutdown this particular connection. If the attacker sends a packet by spoofing a machine, this will have no particular incidence for the compromised spoofed machine.

## References

- Aggressive Network Self-Defense (2005) Syngress Publishing
- Dressler J (1995) Understanding criminal law, 18.02, In: Garland N (ed.) 2nd ed. Fontana, London, pp 199–200
- Méthode, INRA éds. Paris 1997.
- Comment l'ordinateur transforme les sciences, les cahiers de Science et Vie, numéro 53, Octobre 1999.
- Information Operations, Lieutenant Colonel Jordan, US Marine Corps, Active defense (source: scholar.google.com), pp. 50–57
- Karnow CEA (2004–2005) Launch on warning: aggressive defense of computer systems, Yale J law Technol 7:87
- Model Penal Code 3.04(2)(b)(ii)
- NMAP software : [www.insecure.org](http://www.insecure.org) 2005
- [www.legifrance.gouv.fr](http://www.legifrance.gouv.fr) translated with the participation of John Rason SPENCER, Professor of Law, University of Cambridge, Fellow at Selwyn College, UK
- Ossir mailing list, [www.ossir.org](http://www.ossir.org), 2005