12-3-2012

Protective Emblems in Cyber Warfare

Iain Sutherland
Noroff University College

Konstantinos Xynos
University of Glamorgan

Andrew Jones
Khalifa University of Science, Technology & Research

Andrew Blyth
University of Glamorgan

Recommended Citation

Sutherland, I., Xynos, K., Jones, A., & Blyth, A. (2012). Protective Emblems in Cyber Warfare. DOI: https://doi.org/10.4225/75/57a84485befb2

DOI: 10.4225/75/57a84485befb2
13th Australian Information Warfare and Security Conference, Novotel Langley Hotel, Perth, Western Australia, 3rd-5th December, 2012

PROTECTIVE EMBLEMS IN CYBER WARFARE

Iain Sutherland[1,2,3], Konstantinos Xynos[2], Andrew Jones[2,3,4] Andrew Blyth[2]
[1,]Noroff University College, Kristiansand, Norway.
[2] University of Glamorgan, Treforest, Wales, UK.
[3] SRI -Security Research Institute, Edith Cowan University, Perth, Australia
[4] Khalifa University of Science, Technology & Research (KUSTAR) Abu Dhabi, UAE.
Iain.sutherland@noroff.no, kxynos@glam.ac.uk, Andrew.jones@kustar.ac.ae, ajcblyth@glam.ac.uk

Abstract
The Tallinn Manual will be released in February 2013 and makes a significant step towards defining the concepts of cyber warfare. The early draft of the manual is available and the expert working party have interpreted the existing international agreements, instruments and conventions and applied them to the field of cyber warfare. The manual makes a number of interpretations on the legal position of civilians and other parties. The manual makes it clear that the existing conventions are applicable and that civilian / religious and medical systems should be viewed as non-combatants in a cyber conflict. In the kinetic warfare environment non-combatants are indicated with recognized international symbols such as the Red Cross, Red Diamond and the Red Crescent emblems. This paper proposes a simple method in which these and other symbols for protected sites could be replicated in the cyber world with a form of digital marker to ensure that systems and traffic are recognized as being clearly protected under the same terms as those that apply to the Geneva Conventions.

Keywords
Cyber Warfare, Humanitarian Law, Geneva Conventions, Emblems.

INTRODUCTION

There has been considerable debate on the nature of cyber warfare, but general agreement that it does not take place in a legal vacuum, accepted military doctrine such as the UK Joint Service Manual of the Law of Armed Conflict (JSP 383, 2004) can be applied and existing international agreements apply to acts in cyberspace (Rauscher & Korotkov, 2011, Melzer 2011, Dörmann, 2004). Indeed this is the basis for the extensive work in developing the Tallinn Manual (Schmidt 2012). However there are still a number of aspects that require further debate and legal codification.

One of the issues highlighted is the protection of certain individuals, facilities and institutions during a conflict. In kinetic warfare there are a number of entities that are entitled to use an emblem to indicate that they are protect by one or more agreements or conventions. Initially these related to medical symbols agreed in the Geneva International Conference of 1863, (the Red Cross, and later, the Red Crescent and Red Diamond) but also emblems to indicate religious or cultural significance and signs to indicate hazardous sites (International Committee of the Red Cross: The History of the Emblems, 2007). The attack of protected entities is considered a war crime.

> *Pursuant to Article 8(2)(b)(xxiv) and (e)(ii) of the 1998 ICC Statute, "[i]ntentionally directing attacks against buildings, material, medical units and transport, and personnel using the distinctive emblems of the Geneva Conventions in conformity with international law" constitutes a war crime in both international and non-international armed conflicts.*
>
> (International Committee of the Red Cross: Practice Relating to Rule 30)

The use of an emblem by a protected entity is not mandatory; if it is not used then the entity is still protected by the agreements and conventions. Current interpretation suggests that the same rules should be applied to cyber warfare, in that the entities should receive the same protection during a cyber conflict. Therefore there have been a number of suggestions that there is a need for humanitarian emblems to be replicated in cyberspace (Rauscher & Korotkov, 2011, Schmidt 2012) to aid in the identification of entities that should not be targeted.

> *"Therefore, it is essential to bear in mind that, to the extent persons, objects, and activities benefit from the protection of the law of armed conflict generally, they will equally enjoy such protection with regard to cyber operations and attacks."*
>
> (Tallinn Manual p.166) (Schmidt 2012)

There is still significant discussion required on the most effective way to implement these conventions at a technical level, to determine how humanitarian protection might be applied during a cyber conflict (Rauscher & Korotkov, 2011, Schmidt 2012). This paper examines some of the requirements and recent guidance on cyber warfare and examines the problems and technical issues and makes a simple proposal on emblem use in cyberspace.

Targeting issues - what is a legitimate target?

The Tallinn Manual along with a number of other documents (Hathaway *et al* 2011, Rauscher & Korotkov, 2011) have proposed definitions on what does and does not constitute a legitimate target in Cyberspace. Rule 38 of the Tallinn Manual describes civilian objects and military objectives, which may include computers, computer networks and cyber infrastructure. Overall a number of rules cite the need to distinguish between Civilian and Military targets. Although there are circumstances where targets may have dual use. One example of dual use is where a network carries both Civilian and Military traffic. This is currently considered to be a legitimate Military target, Rule 39.

> *RULE 32 – Prohibition on Attacking Civilians*
>
> *The civilian population as such, as well as individual civilians, shall not be the object of cyber attack.*
>
> *5" To qualify as the object of an attack, the harm to the relevant person (or object) must meet the level set forth in Rule 30. For instance, consider the case of a cyber operation intended to harm a particular individual by manipulating her medical information stored in a hospital's database. She would be the object of attack, but the database would not be if the damage thereto does not rise to the level required for an attack. "*

Note that Rule 38 in relation to civilian objects and military objectives, states that civilian objects that make a contribution to military action are considered as legitimate targets (military objectives) including computer networks and infrastructure. It highlights the fact that although messages are of military concern, the legal interpretation is that it is the network hardware that is the military objective. Further legislation may be needed to clarify the legal status of data although the infrastructure is clearly a legal target. Rule 38, point 10 suggests that if a civilian object has become a military objective through participating in a conflict, it can revert to civilian (non-combatant) if it is no longer involved in the conflict. This is where marking traffic may help to indicate use and examining traffic will help to provide an indication of the network use. There is an in issue of granularity as what timescale would need to be considered for a network to revert to civilian after carrying military traffic.

There is a requirement to encode multiple emblems in such a way as they can be easily identified and to provide methods for the emblem information to be presented to clearly identify the protected status of the system or data to the attacker. It would require a system that was able to emulate the protection provided to the different emblems chiefly: medical, religious and cultural.

> *"RULE 71 – Medical Computers, Systems, and Computer Networks*
>
> *Computers, computer networks, and data that form an integral part of the operations or administration of medical units and transports must be respected and protected, and in particular may not be made the object of attack."*
>
> *"4. If the objects referred to in this Rule are also being used to commit, outside their humanitarian functions, acts harmful to the enemy, they lose their protection against attack, subject to Rule 73.* ***This situation is particularly relevant in the cyber context because medical data can be stored in the same data centre, server, or computer as military data."***
>
> (Tallinn Manual), (Schmidt 2012)

The necessity of protecting medical data systems is clear and it is easy to illustrate the requirements for religious communications. Examples of cultural systems may include digitised repositories of artifacts and even archived social media (SalahEldeen &. Nelson 2012).

Tactical concerns

The attacker needs to be able to identify that the emblem is present without indicating the possibility of an imminent attack. For instance if a system returned a value from a specific port on a machine indicating status as a protected system, then the act of probing this port may indicate to the owner that some form of cyber attack on that network or area is imminent.

There is some suggestion that a cyber attack on an individual medical record is legal, if belonging to an armed forces individual? As Rule 32:5 (above) implies the legality of modifying medical data in an attack, however individuals under medical care in a conflict zone normally have the same protection as the hospital itself; they are considered non-combatant. Also how would scanning a hospital network to gather intelligence on wounded and captured personnel prior to a rescue be viewed? The Tallinn Manual suggests that, in that same way a network may be attacked due to the transport of military information then a PC can be attacked due to the contents of a file folder or database based on if it is supporting military action. This means it would be unwise to permit the storage of civilian / medical and military information on the same system. This is contrary to the current trend to store data in cloud systems. There is the clear need to separate out civilian objects and military objectives. It is possible to achieve this by clearly separating hardware and storing it in different locations. It is another matter altogether when taking into consideration networks that have to route information based on algorithms that operate to deliver packets using the shortest path. The separation of network data to protect civilians in the event of a cyber conflict in practice is difficult to achieve or unfeasible, as this would require completely separate networks for civilian and military traffic. One of the defining characteristics of cyberspace is the interconnected nature of systems this is highlighted in the complex interdependencies of a Critical National Infrastructure. Military and Civilian infrastructures often rely on the same or related power and water distribution networks (controlled by the same information infrastructure). In a similar fashion they may transport information on the same computer based networks, or store data within the same data center.

A suitable solution would make it possible to clearly identify a Hospital computer, a brigade Chaplin's laptop, a water purification plant, a nuclear power station, to enable the existence of these systems to be taken into consideration when assessing military objectives. There is of course the possibility that a site containing dangerous forces e.g.: a dam could be considered a target although this is based on the military objectives when planning an attack.

There is the issue that a marking system could be open to abuse, the same as the emblems are in kinetic warfare. The misuse of these emblems in kinetic warfare is referred to as perfidy and is considered a war crime. It may be that a possible solution can address this technically. There is also the risk of a system owner committing perfidy unintentionally in the digital environment . If systems are automatically allocating an emblem to network traffic any system labeling the packets would need careful oversight. There is also the issue that a system could be identified by attacker not concerned with adhering to the Geneva Convention or with the potential of committing a war crime. The issue of the system being highlighted to e.g terrorist groups that may be facilitated in finding a target with such a system.

Technical issues

Despite the potential issues there is a clear need for both systems and data to be marked with protective emblems to indicate their non-combatant status. We propose the following methods for marking a digital system:

- The use of the Top Level Domains of systems (TLD) to indicate network / IP address with protected status
- The use of TCP/IP packet marking to indicate a protected packet traversing a network
- The use of a Warning screen to indicate protected status of systems / applications

Top level domain

One suggestion has been made for protected organizations is the introduction of a Top Level Domain (TLD) specific to protected sites (Rauscher & Korotkov, 2011). The creation of a TLD marker then can be used to register systems. The most obvious would be the use of .MED to designate a medical network. This solution would provide the necessary separation of systems and networks required to prevent a civilian system becoming 'collateral damage' in a cyber attack. However if any form of NAT (Network Address Translation) is being used as part of a network then it will not be possible to identity a protected system or to ensure that the clear designation of a protected packet of data coming from a particular system.

The use of a TLD may indicate a particular type of system. This could highlight the nature of the system as a target to terrorists, but then IP ranges are available and other open source information can help identify these networks. The use of the TLD merely makes it explicit.

Warning banner

Individual Systems and applications may also be marked to indicate protected status. It is a common security practice to place a warning banner on systems or applications at the point of login to discourage an intruder and to provide and demonstrate unequivocal clear intent on the part of and that an intruder knew that further unauthorized access would be illegal. Typically this would include reference to Data Protection and Computer Misuse legislation. See figure 1 for an example from the UK.

```
This system is for authorised users only.
Unauthorised users will be subject to prosecution
Section 1 Computer Misuse Act 1990
Data Protection Act 1989
```

Figure 1: Warning Banner

There may then be some value, if the system is eligible for a protective emblem, for the inclusion of text that highlights this to a potential cyber attack. A suggested banner is shown in figure 2.

```
"This system bears the digital emblem of the ICRC. Intentionally directing
  cyber attacks again this system or the data contained within may be a
breach of the Geneva Conventions, international law and may constitute a
                          War Crime"

(Article 8(2)(b)(xxiv) and (e)(ii) of the 1998 ICC Statute)
```

Figure 2: Example Cyber Attack Warning Banner

Packet markers

Although the exact legal status of data appears unclear and possibly requiring additional legislation, which is outside of the remit of this paper, it is the data, in the form of network traffic, which a cyber attacker will interact with or generate during an attack. In a similar way to a physical medical convoy being marked in transit through a battle zone with ICRC emblems, a cyber attacker when faced with network traffic and particularly machines as potential targets indicated as being used for humanitarian purposes, must be able to factor this into his decision to attack the network or the system.

These markers (or emblems) can be a deterrent from having attackers either attack a particular network, as it is clear which traffic is of protected civilian use and which of military. The protection would be that stated in the Geneva Convention. Such markers can only be made possible by including special detail into packets crafted by the machines connected to the networks. This information should be easily communicated across the different domains and systems it traverses clearly stating that the traffic is of civilian use and should be allowed.

We propose that considerations be made at a number of levels to consider a wider adoption of special markers in network traffic that would enable protectively marked traffic to be easily visible in network flows. These markers can exist at different layers of the OSI model.

If traffic is marked as protected then it is also easier to allow or even block this traffic based on simple rules. This would make it easier for military operations to be carried out without having to take down whole networks that would have a mixture of traffic.

It is proposed that special civilian markers are made available at least at the network layer (layer 3) of the OSI model. This can then be further extended into having redundant information stored in the transport layer (layer 4).

The majority of traffic that traverses networks makes wide use of the IPv4 header (layer 3). Therefore there is the ability to propose that parts of the OPTIONS field (see figure 3) are used, these could be extended to contain the proposed additional data an encoding of the Humanitarian emblems.

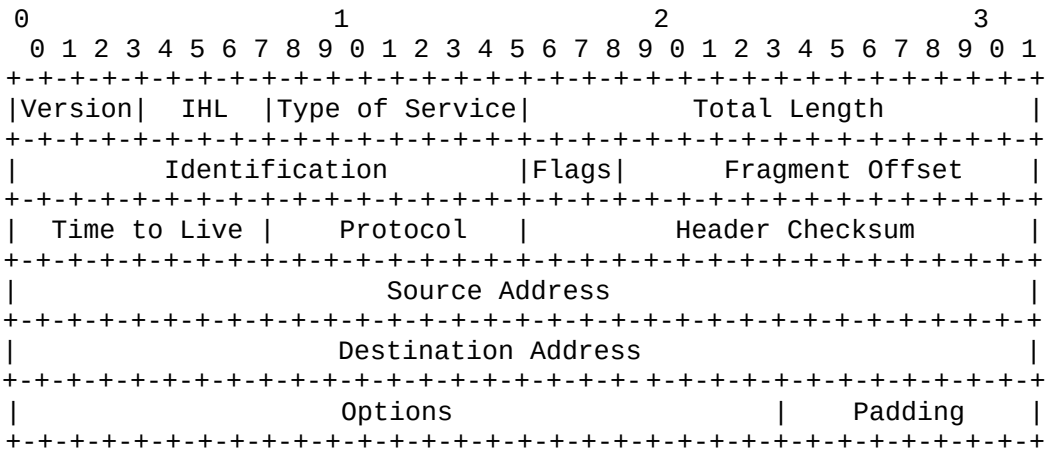

Figure 3: Example Internet Datagram Header (RFC 791)

According to RFC 791 the options field can hold either a single Octet defining an option type or an options type with an option length and associated option data. Specific types are defined in RFC 791 and further extended by a list published by IANA (Internet Assigned Numbers Authority, 2012a).

Within RFC 791 there is a security option which allows for the clear classification of traffic for military purposes. In a similar way, we propose a new option's field that would have 1 octet (or 1 byte) for the type field with a type number above 190. The length of the options field should be variable with a minimum set at 5 octets and therefore it should also have the ability to support any future extend functionality via the extended options. As part of the options data an embedded 2 octet emblem will be included clearly stating a humanitarian emblem.

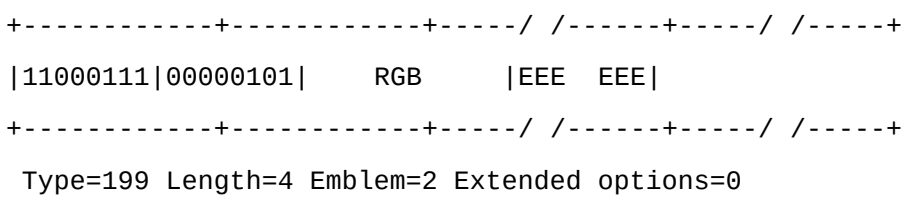

Figure 4: Example of Proposed Humanitarian Emblem IPv4 Option

The type should have to be easily distinguishable from the security ones that are defined, those found in the 130 range. This also ensures that if the military makes use of these fields then an analyst can clearly see the difference, thus avoiding any possible confusion. It is suggested that the pattern produced by the option type 199, in binary, also recreates a close resemblance to the universally recognised Morse code for SOS in binary, 111000111, with its most significant bit missing to fit the 8 bit octet and therefore should be considered as a candidate.

The emblem field can have an encoding allowing for further processing at a later stage. The encoding is based on the format used to represent 1 pixel in as defined by device independent bitmap (DIB) file format, also widely known as BMP file format based on a 16 bit RGB colour representation.

Therefore the binary 00001000 00000000 could be used to indicate an ICRC emblem in binary form. This would translate into the 16 bit RGB colour representation of red being, A0000: R1000: G0000: B0000, where A is alpha, R is red, G is green and B is blue.

There are some drawbacks to this system as it would duplicate the symbol as it is used in a kinetic warfare environment, in that the system is open to perfidy. There is no proof of authenticity. The field can be duplicated

/copied or inserted into any packet. This would be the equivalent of committing perfidy in a kinetic conflict. There is also the effect of adding additional data into each packet and the resulting effect on network performance. However, this does provide a consistent and simple method of labeling traffic.

The addition of further data into the option field could enhance this from simply replicating the marking of an emblem in cyberspace to providing some measure of confidence in the contents. It must be noted that the options field of an IP header has a maximum length of 320 bits (40 bytes) of data and as options are used on a daily basis relevant considerations should be made before any large extensions are made to the field.

With the wider adoption of IPv6, RFC2460, there is a need to mention that the proposed header can very well be specified for IPv6 packets. The main issue that would have to be put forward to the community would be the limitation imposed by the RFC in examining or processing headers as they pass through nodes. There is an exception put forward for the Hop-by-Hop Options header, which means that the community is willing to consider exceptional circumstances

The authors are aware that this proposal is limited to the protocols mentioned and networks operate at a more complex level. This is even more evident when a mixture of protocols comes into play and protocols are encapsulated leading the markers being hidden. These issues will have to be addressed by the individual working groups.

To implement these changes would require a number of measures. An update to the current RFCs in question would be required to formally document the specific requirements of the options field. As well as further international legal agreements are required to clarify the position of data within a cyber conflict.

CONCLUSIONS

This paper examines the concept of cyber warfare and the need for protective signs indicating individuals or locations that should not be attacked to be replicated in a cyber environment. We acknowledge that legislation still needs to be clarified on certain aspects of cyber conflict. However we propose the following practical system may be useful for marking aspects of a cyber environment to ensure that the protected nature of certain aspects is clear: The use of a Top Level Domains to indicate a block of IP addresses with a protected status and the use of a system to indicate a protected TCP/IP packet traversing a network and the use of banner / warning screen for systems / applications to indicate protected status.

REFERENCES

Dörmann, K. (2004) "The Applicability of the Additional Protocols to Computer Network Attacks: An ICRC Viewpoint", in K. Byström (ed.), Proceedings of the Conference: International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, 17–19 November 2004, Stockholm, Sweden, 2004, pp. 139–53.

Also Available online at:

http://www.icrc.org/eng/assets/files/other/applicabilityofihltocna.pdf

Hathaway O.A., Crootof R., Levitz P., Nix H., Nowlan A Perdue W., Spiegel J., (2011) The Law of Cyber-attack. California Law Review, Vol. 100, No. 4, 2012.

International Committee of the Red Cross: Resolutions of the Geneva International Conference. Geneva 26-29 October 1863. http://www.icrc.org/ihl.nsf/FULL/115?OpenDocument

International Committee of the Red Cross: The History of the Emblems (2007) http://www.icrc.org/eng/resources/documents/misc/emblem-history.htm

Internet Assigned Numbers Authority (2012a), 'IP Option Numbers' http://www.iana.org/assignments/ip-parameters/ip-parameters.xml

Internet Assigned Numbers Authority (2012b), 'IPv6 Parameters' http://www.iana.org/assignments/ipv6-parameters/ipv6-parameters.xml

JSP 383 (2004) The Joint Service Manual of the Law of Armed Conflict. http://www.mod.uk/NR/rdonlyres/82702E75-9A14-4EF5-B414-49B0D7A27816/0/JSP3832004Edition.pdf

Manual on International Law applicable to Air and Missile Warfare 2009. Program on Humanitarian Policy and Conflict Research at Harvard University http://www.ihlresearch.org/amw/aboutmanual.php

Meltzer N, (2011) Cyber operations and Jus in Bello Disarmament forum, Confronting Cyber conflict. http://www.unidir.org/pdf/articles/pdf-art3164.pdf

RFC2460 Internet Protocol, Version 6 (IPv6) Specification http://www.ietf.org/rfc/rfc2460.txt

RFC791 Internet Protocol, DARPA Internet Program, Protocol Specification, September 1981. http://www.ietf.org/rfc/rfc791.txt

Rauscher K.F. Korotkov, A (2011) The Russia-U.S. Bilateral on Critical Infrastructure Protection Working Towards Rules for Governing Cyber Conflict Rendering the Geneva and Hague Conventions in Cyberspace. (Issue 1) An advance publication of this paper was presented at the Munich Security Conference, February 4-6, 2011. EastWest Institute.

SalahEldeen,H.M. Nelson M.L, (2012) Losing My Revolution: How Many Resources Shared on Social Media Have Been Lost? Theory and Practice of Digital Libraries, Lecture Notes in Computer Science Volume 7489, 2012, pp 125-137

Schmitt M. N. (Editor) (2013) Tallinn Manual on the International Law Applicable to Cyber Warfare. The NATO Cooperative Cyber Defense Centre of Excellence, Cambridge University Press. 2013 http://issuu.com/nato_ccd_coe/docs/tallinn_manual_draft?mode=window&backgroundColor=%23222222

Schmitt M. N., Garraway C.H.B., Dinstien .Y., (2006) The San Remo Manual on the Law on Non-international Armed Conflict with Commentary. International Institute of Humanitarian Law http://www.iihl.org/iihl/Documents/The%20Manual%20on%20the%20Law%20of%20NIAC.pdf

[tcpm] TCP options - tcp-parameters IANA registry http://www.ietf.org/mail-archive/web/tcpm/current/msg03199.html