

This article was downloaded by: [US Army War College]

On: 01 October 2014, At: 07:22

Publisher: Routledge

Informa Ltd Registered in England and Wales Registered Number: 1072954 Registered office: Mortimer House, 37-41 Mortimer Street, London W1T 3JH, UK



The RUSI Journal

Publication details, including instructions for authors and subscription information:

<http://www.tandfonline.com/loi/rusi20>

War by Analogy

Jody Prescott

Published online: 22 Dec 2011.

To cite this article: Jody Prescott (2011) War by Analogy, The RUSI Journal, 156:6, 32-39, DOI: [10.1080/03071847.2011.642683](https://doi.org/10.1080/03071847.2011.642683)

To link to this article: <http://dx.doi.org/10.1080/03071847.2011.642683>

PLEASE SCROLL DOWN FOR ARTICLE

Taylor & Francis makes every effort to ensure the accuracy of all the information (the "Content") contained in the publications on our platform. However, Taylor & Francis, our agents, and our licensors make no representations or warranties whatsoever as to the accuracy, completeness, or suitability for any purpose of the Content. Any opinions and views expressed in this publication are the opinions and views of the authors, and are not the views of or endorsed by Taylor & Francis. The accuracy of the Content should not be relied upon and should be independently verified with primary sources of information. Taylor and Francis shall not be liable for any losses, actions, claims, proceedings, demands, costs, expenses, damages, and other liabilities whatsoever or howsoever caused arising directly or indirectly in connection with, in relation to or arising out of the use of the Content.

This article may be used for research, teaching, and private study purposes. Any substantial or systematic reproduction, redistribution, reselling, loan, sub-licensing, systematic supply, or distribution in any form to anyone is expressly forbidden. Terms & Conditions of access and use can be found at <http://www.tandfonline.com/page/terms-and-conditions>

WAR BY ANALOGY

US CYBERSPACE STRATEGY AND INTERNATIONAL HUMANITARIAN LAW

JODY PRESCOTT

The recent exponential growth in cyber-attacks against the digital infrastructure of governments, economies and militaries has potentially catastrophic effects. To date, however, governments are still trying to formulate strategic responses to this new threat. The development of a legal and policy framework consistent with international humanitarian law is essential to the successful creation and implementation of a strategy for operating in cyberspace.

The use of cyberspace for unfriendly purposes by often unidentifiable actors against military, industrial and governmental digital infrastructure has grown exponentially in recent years. Events such as the infection of Iranian nuclear facilities by the Stuxnet worm, the recent disclosure of the theft of information from over seventy US and international organisations and corporations during a five-year period by an unnamed state actor,¹ and the disruption of Georgian governmental services and communications during its war with Russia are among the more prominent examples of cyberspace actors' malicious behaviour. The US Department of Defense (DoD) has stated that its computer systems are scanned by potentially hostile actors over a million times a day and actually probed over a thousand times daily.² In discussing attacks on NATO computer systems, NATO Secretary General Anders Fogh Rasmussen has stated: 'It's no exaggeration to say that cyber-attacks have become a new form of permanent, low-level warfare'.³

The secretary general's assessment does not capture the full extent of the threat posed by malicious actions in cyberspace, however. This level of ill-intended activity, coupled with the great dependence of modern post-

industrial states upon reliable, capable and accessible digital infrastructure, creates pronounced risks to the functioning of governments, economies and militaries. Exploitation of national and international network vulnerabilities by malicious actors has the potential for catastrophic effects that would ordinarily result only from the use of armed force on a significant scale.⁴ Not surprisingly, technologically advanced militaries and civilian governmental agencies are continuing to develop capabilities to operate offensively in cyberspace.⁵ The United States' assessment is that more than thirty 'countries are creating cyber units for their militaries'.⁶ Also, not surprising given the rapidity of cyber-technology advances, the development of the legal and policy constructs consistent with international humanitarian law (IHL), which would guide the proper use of these capabilities, appears to have lagged behind.⁷ The lack of doctrine in these respects is of grave concern internationally, and many nations, non-governmental organisations and academics have begun the difficult work of identifying practical, sustainable solutions to these gaps.⁸

In 2011, the US released four documents that deal with the use of force in cyberspace: the Obama administration's International Strategy

for Cyberspace (hence International Strategy), published on 16 May; the DoD's Strategy for Operating in Cyberspace (DoD Strategy), published on 14 July; a report by the US Government Accountability Office (GAO), Defense Department Cyber Efforts (Cyber Efforts report), released 26 July; and finally, the DoD Cyber Policy Report, made public on 14 November. To help identify the degree to which these documents provide insight into the US approach to applying IHL in cyberspace, this article will first address the more significant legal and policy issues regarding the use of force in this domain. Secondly, it will briefly review each of these documents in turn, to identify the issues they raise regarding the application of IHL. Lastly, this article will describe different ongoing US cyber-efforts and programmes, the conduct of which might help achieve a better understanding of how IHL actually applies to the use of force in cyberspace.

Cyberspace Legal and Policy Issues

Are all military actions in cyberspace uses of armed force?

Pursuant to the processes established to complete the work of defining the jurisdiction of the International Criminal Court, the Rome Statute was recently



US Air Force cyber-security personnel at Barksdale Air Force Base, Louisiana. Photo courtesy of Department of Defense/Cecilio Ricardo.

amended to include a definition of the criminal act of aggression. Aggression is defined as 'the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any manner inconsistent with the Charter of the United Nations'. Examples of aggression include the use of armed forces to invade another country, bombard it or blockade it.⁹ In contrast, very unfriendly and injurious acts of states against each other, such as diplomatic coercion and trade embargoes, have not historically been seen as uses of armed force and therefore are not defined as acts of aggression.¹⁰ Mere espionage has not been seen as a war-like act traditionally, despite its hostile nature.¹¹ Even uses of armed force below a certain threshold do not appear to be regarded by states as constituting armed conflict.¹² For example, the recent accidental 'invasion' of the US by Mexican Army forces does not appear to have been considered an act of war by either country.¹³

What is the appropriate standard for responding in self-defence?

There is significant international disagreement as to the scope of the

right of self-defence under Article 51 of the UN Charter. Two particular points of disagreement are how imminent an armed attack must be before a state may respond in self-defence,¹⁴ and whether a state might respond in self-defence against the war-like acts of a non-state actor.¹⁵ The degree of probing of DoD systems by unfriendly actors as described previously might, from the perspective of a cyber-defence operator, look like continual attack, carrying with it the possibility of serious attack. At the moment of identification, it might be impossible to determine either an unauthorised intruder's identity or intent. Because of the speed at which it could move from exploitation to destruction, however, any intrusion could pose a very serious threat. The issue is further complicated by the very significant degree to which military cyber-systems rely upon civilian digital infrastructure to operate, and unresolved questions remain as to who is responsible for responding to cyber-incidents, within which legal and policy framework and with which tools.¹⁶ For example, the US Department of Homeland Security (DHS), which is responsible in large part for US civilian security issues and

has its own National Cybersecurity and Communications Integration Center, has signed a memorandum of agreement with the DoD to co-ordinate cyber-activities and the use of personnel between the agencies. Despite the very practical reality of military and civilian cyber-interdependence, however, the agreement notes that 'existing DoD and DHS authorities, command relationships, ... privacy, civil liberties, and other oversight relationships' remain unaltered.¹⁷

Would a state's failure to prevent the misuse of digital infrastructure assets on its territory infringe its neutrality?

Under international law, neutral states have an obligation to safeguard their neutrality and prevent their territory from becoming a launch pad for attacks by one state against another. If neutral states fail to prevent serious misuse of their territory or are unwilling to prevent it, then the party attacked from the neutral state's territory could consider the neutral state a co-belligerent and engage the enemy forces.¹⁸ Given that sophisticated cyber-actors are capable of effectively hiding their true identities

in the anonymity of cyberspace, or 'spoofing' so that they appear to be entities of benign intent, the actual launch site of an attack against a network might in fact be completely unrelated to the attacker, and the government of the state in which the server sits in the physical world might be completely unaware of the attack.

US DoD systems are probed over a thousand times daily

If the effects of cyber-actions ripple into the physical world, how accurately can incidental damage be estimated?

Under IHL, attacks may be conducted so long as the 'concrete and direct military advantage' anticipated is not excessive in relation to the 'incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof'.¹⁹ As a matter of policy, rules of engagement will often restrict a commander's discretion in how this balance is calculated, as shown by the 'Tactical Guidance' issued by the ISAF commander to subordinate forces in Afghanistan.²⁰ Importantly, however, the application of proportionality under IHL is not the same as the proportionality analysis that a law enforcement agent would conduct under domestic laws of self-defence. Irrespective of which legal and policy standards apply, there are complex technical issues that bear on the propriety of engaging in an attack under IHL as well. Even in the physical world, there remain important questions as to the boundaries of the scope of the information on potential civilian damage and injury a commander must consider in deciding whether to engage, and what sort of technologies collecting this information can be properly synchronised with staff processes to make this information available to a commander when needed. It may be that computer modelling of proposed actions in cyberspace exists, to provide a commander with an accurate picture of where the effects of these actions would ripple into the physical world, so that more typical reconnaissance assets

could be employed to assess the 'pattern of life' at these locations and allow the commander to assess accurately potential damage to protected persons and property. However, if it does exist it is likely classified and thus difficult to debate in the public domain.

The International Strategy for Cyberspace

The first section of the International Strategy, 'Building Cyberspace Policy', defines the overall US strategic approach as being grounded in three principles: fundamental freedoms, privacy and the free flow of information.²¹ This is in marked contrast to what is seen by certain Chinese writers as being essential: the maintenance of 'Internet borders' and the protection of 'Internet sovereignty'.²² This contrast between the US view of cyberspace as being part of a 'Global Commons' and the Chinese view, which emphasises national sovereignty, is also reflected in the two nations' respective views of the oceans and space.²³ As to fundamental freedoms, the strategy sees 'the ability to seek, receive and impart information and ideas through any medium' as an internationally recognised civil liberty. 'Privacy' is defined in terms of a balance between individuals' expectations as to how their personal data would be used fairly and protected, and the concurrent prevention of criminal activity against personal information through regulated law enforcement actions. The strategy defines the principle of 'the free flow of information' as the favouring of an information exchange environment which is 'a level playing field that rewards innovation, entrepreneurship, and industriousness, not a venue where states arbitrarily disrupt the free flow of information to create unfair advantage'.

In line with these basic principles, the second section of the strategy describes the end state the US wishes to achieve through international action:²⁴

An open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression

and innovation. To achieve that goal, we will build and sustain an environment in which norms of responsible behavior guide states' actions, sustain partnerships, and support the rule of law in cyberspace.

This is important to the US because it believes a gap has grown between 'governments seeking to exercise traditional national power through cyberspace' and 'clearly agreed-upon norms for acceptable state behavior in cyberspace'. In addressing this gap, the US believes that the 'long-standing international norms guiding state behavior – in times of peace and conflict – also apply in cyberspace', but that the 'unique attributes of networked technology require additional work to clarify how these norms apply and what additional understandings might be necessary to supplement them'. The US sees the building of consensus to identify these norms as requiring neither 'a reinvention of customary international law' nor the rendering of 'existing international norms obsolete'.²⁵

In terms of existing norms, the strategy affirms that 'consistent with the United Nations Charter, states have an inherent right to self-defence that may be triggered by certain aggressive acts in cyberspace'. Interestingly, the International Strategy also sets out what it describes as emerging norms essential to the proper use of cyberspace, including 'Cybersecurity Due Diligence', which it defines as the obligation of states to protect their 'information infrastructures and secure national systems from damage or misuse'.²⁶ Potentially, the concept of cybersecurity due diligence could provide a basis for US forces to reach into a neutral state's cyberspace and conduct cyber-operations, active defence or otherwise, if the neutral state had not been policing its cyberspace sufficiently to prevent an attack by third state or even non-state actors. Left unanswered in the International Strategy are questions as to who decides whether a state has been sufficiently diligent to remain neutral and its cyberspace therefore inviolable, and what standards would be used to make this decision.

To attain its end state, the strategy also sets out diplomatic, development and defence objectives. The accomplishment of the defence objective is likely to prove the most challenging in developing consensus as to the applicable legal norms – the use of force in cyberspace. In prefacing the defence objective, the strategy notes that the US ‘will defend its networks, whether the threat comes from terrorists, cybercriminals, or states and their proxies ... [using] a range of credible response options’. The objective of such defence is to, ‘along with other nations, encourage responsible behavior and oppose those who would seek to disrupt networks and systems, dissuading and deterring malicious actors, and reserving the right to defend these vital national assets as necessary and appropriate’. Although the dissuasion element of the defence objective is phrased in positive terms, as it describes the fostering of a robust cyber-defence capacity both in the US and abroad, the deterrence element is described much more plainly. In operating pursuant to this element, the US states that it ‘will ensure that the risks associated with attacking or exploiting our networks vastly outweigh the potential benefits’. It recognises ‘that cyberspace activities can have effects extending beyond networks; such events may require responses in self-defence’.²⁷

In conclusion, the International Strategy notes:²⁸

When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country ... and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners ... We reserve the right to use all necessary means ... as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests.

Of course, the actual rules of engagement for cyberspace for all state actors that have offensive cyber-capabilities are likely classified and therefore can only be discussed speculatively in the public

domain. Nevertheless, the use of the phrase ‘hostile act’ in the International Strategy is probably intentional, and it would conceivably allow a more robust US response than would be allowed under NATO rules of engagement, for example, which use the same phrase but define it in a more restricted fashion.²⁹ Further, the US’s position that the use of armed force in the physical world is a potentially appropriate response to a cyber-attack raises the question of whether a higher standard of attribution would be required for such use, where there was not already an ongoing armed conflict in the physical world. This could lead to looking at action involving both cyberspace and the physical world as being akin to a game of multidimensional chess, but with different rules being applied at the same time depending upon the level on which the pieces are moving.

DoD Strategy for Operating in Cyberspace

Released two months after the International Strategy, the unclassified version of the DoD Strategy is perhaps most remarkable for what it does not say. There is no mention of offensive cyber-capabilities, nor is there any discussion of the way in which IHL is to be implemented in cyber-operations. Instead, the strategy sets out five complementary strategic initiatives which emphasise the importance of creating a well-organised, trained and equipped cyber-force structure; partnerships with civilian governmental agencies, private industry, allies and other international partners; and developing a national wellspring of talent and innovation to keep the US military and industry competitive in the cyber-arena. Only one of the initiatives, ‘Employ new defense operating concepts to protect DOD networks and systems’, has any content that deals with the potential use of armed force in cyberspace.³⁰ Even this initiative, however, is focused inward on the DoD systems themselves, and it highlights the importance of cyber-hygiene to minimise opportunities for intrusion into the systems, and increased oversight and accountability of the workforce regarding the use of DoD networks and systems.³¹

The only aspect of this initiative that hints at an effort to increase the resilience of DoD networks and systems through the use of more forceful measures is the employment of ‘active cyber defence’ as an operating concept. The DoD Strategy defines active cyber-defence as ‘synchronized, real-time capability to discover, detect, analyze and mitigate threats and vulnerabilities’. Taken alone, this language could seem rather innocuous. What it does not specify, however, is where an active cyber-defence would be looking to discover threats, how they are to be analysed, and most importantly, the range of effects considered ‘mitigating’.³² Statements attributed to unidentified US officials suggest that active cyber-defence actually includes intrusion and potential cyber-action in other states’ digital infrastructure.³³ Such actions could conceivably violate longstanding legal and policy norms regarding state sovereignty. If in fact the US concept of active cyber-defence means that military means would be used to seek malicious code on servers in other countries, and potentially delete it once found, the most pertinent question is whether this would be sufficient to trigger the international legal norms regarding the use of armed force. Further, active cyber-defence appears to involve a high degree of automated cyber-response,³⁴ which raises issues of whether and where a human commander exercises appropriate command responsibility for these targeting decisions in the decision chain.

There is no mention of offensive cyber-capabilities

The DoD Cyber Policy Report

The mildness of the DoD Strategy was even more surprising given statements made by Obama administration officials in the weeks prior to its release that suggested that it would set out a new concept of ‘equivalence’ between war-like acts in the physical world and those that happen in cyberspace.³⁵ In

the absence of such discussion, ranking members of the US Senate Committee on Armed Services immediately reminded the secretary of defense that the DoD had agreed to provide a report to the committee by the end of 2010, addressing 'a number of critical questions, including the relationship between military operations in cyberspace and kinetic operations; ... the rules of engagement for commanders; the definition of what would constitute an act of war in cyberspace; and what constitutes the use of force for the purpose of complying with the War Powers Act'.³⁶ Accompanied by a classified annex, the unclassified report was delivered to Congress on 14 November 2011. The DoD Cyber Policy Report itself dodged most of the specific questions that the DoD had been asked to address, but certain details hint at an outline of the approach that the US might be taking regarding the use of force in cyberspace and the role of IHL.

First, the report focuses on hostile intent, in the form of either actual or implied threats, and hostile acts in cyberspace as the basis for a military response. This conduct-based approach to the use of force would probably not be the preferred method for establishing 'positive identification' as compared to actual attribution; however, the potential significance of this approach is reinforced by the report's disclosure that the US is working to resolve attribution problems in part through the use of 'behavior-based algorithms'.

Second, the report states that hostile acts must be 'significant',³⁷ suggesting that the DoD has perhaps defined or illustrated in the classified annex, through the use of examples, the threshold point past which cyber-annoyance could be considered a cyber-attack. Third, although the report acknowledges the importance of applying IHL when using offensive force in cyberspace, it states that 'other policy principles and legal regimes that [the DoD] follows for kinetic capabilities' are also applicable.³⁸ Presumably, these other 'policy principles and legal regimes' include US domestic law, executive orders and perhaps even military regulations such as rules of engagement. Further, the report notes

that because of 'cyberspace's unique aspects', the role of IHL might 'require clarification in certain areas'.

The current situation is a temporary imbalance in capability and intent

Finally, in two very important areas where the DoD plainly sidestepped the questions posed by Congress – rules of engagement and sovereignty – the report instead provides lists of non-prioritised considerations that would be applied in deciding whether to respond to unfriendly cyber actions with force. In the case of the former, the considerations listed include the speed at which events occur in cyberspace and the need to protect the communications backbone of continuous, worldwide military operations, suggesting that US rules of engagement will likely allow a significant degree of latitude in forceful responses. Similarly, the report lists some very functional considerations pertinent to whether a third country's sovereignty might be infringed by a US cyber action, especially where that country has failed to exercise sufficient cyber-security due diligence. This suggests that the US does not believe that 'sovereignty' as it is understood in the physical world necessarily translates completely in cyberspace.³⁹

Transmission in the Clear

Given the understatement and circumlocution of the DoD Cyber Strategy and the DoD Cyber Policy Report, the best source from which to glean indications of the directions in which the DoD might be moving on these issues are the remarks made by Deputy Secretary of Defense William J Lynn at the National Defense University on 14 July 2011, announcing the launch of the DoD Strategy. Deputy Secretary Lynn first highlighted the broadness of the threat spectrum, ranging from state actors possessing sophisticated cyber-capabilities at one end to opportunistic criminal actors and 'rogue states' at the other. Whilst deterrence might be

effective in preventing major state actors from engaging in destructive cyber-measures against the US, terrorists and rogue states with 'few to no assets to hold at risk' were not likely to be dissuaded by the same measures. The DoD assessed the current situation in cyberspace as a temporary imbalance in capability and intent. Those with the capability were developing even 'more destructive tools', but were unlikely to use them in the near future. Those with the greatest intent to inflict harm were currently without such means, but would eventually acquire them.

In the future, Deputy Secretary Lynn stated, 'we are likely to see destructive or disruptive cyber-attacks that could have an impact analogous to physical hostilities', however, 'the vast majority of malicious cyber activity today does not cross this threshold'.⁴⁰ The use of 'analogous' to describe the relationship between physical world war-like acts and serious unfriendly acts in cyberspace is interesting. Prior media accounts had reported that a doctrine of 'equivalence' would be set forth in the strategy to describe this relationship.⁴¹ Distinguishing the meanings of words too finely can be misleading, but 'equivalent' suggests a more direct relationship than 'analogous'. This perhaps suggests that the US does not intend to directly import IHL applications and understandings into its legal and policy bases for action in cyberspace. Further, if the US is taking the position that activity analogous to armed conflict is already occurring in cyberspace, then identity and actual intent might not matter so long as it can be determined with reasonable certainty that the actor appears to be committing a hostile act or displaying hostile intent,⁴² as defined under US Standing Rules of Engagement.⁴³ Attribution as a prerequisite for responding with armed force in national self-defence has a higher threshold than if a nation's armed forces were acting in self-defence in a situation of already ongoing conflict, at least under US domestic authorities governing the use of force. Attribution would still be important in these circumstances if a proposed course of action were to attack assets of a state actor that were not related to the intrusion.

As to cyber-conflict itself, Deputy Secretary Lynn noted that public discussion had raised the spectre of the militarisation of cyberspace resulting from the military's attempts to defend a domain that 'was overwhelmingly used by civilians and for peaceful purposes'. In response, he pointed out that although the US reserved 'the right, under the laws of armed conflict, to respond to serious cyber-attacks with a proportional and justified military response at the time and place' of its choosing, the majority of the DoD Strategy was instead focused upon defensive and confidence-building measures, to be achieved through partnerships with civilian government agencies, industry and international allies.⁴⁴ Deputy Secretary Lynn's description of active cyber-defence, however, suggests that the language in the DoD Strategy might not be as defensive as it seems. Active cyber-defence in the DoD Strategy is the use of 'sensors, software, and signatures to detect and stop malicious code before it affects our operations'. This implies a lower threshold for active cyber-defensive action, which in turn suggests the possibility of reaching out beyond the DoD networks to conduct such actions effectively. Conversely, Deputy Secretary Lynn's phrasing, 'impact analogous to physical hostilities', suggests a threshold for military offensive response higher than just the use of military means by an intruder to gain access to US networks and systems. These two thresholds potentially delimit an area in which cyber-snooping to hunt for malicious code in another state actor's networks and systems, for example, is not seen as an act analogous to war. Conceivably though, the action of 'mitigating' malicious code once it is found might be perceived quite differently by the state whose digital infrastructure experiences virtual cleansing.

Defense Department Cyber-efforts

A week after the release of the DoD Strategy, the US GAO released the unclassified version of its report to Congress on the DoD's efforts in the cyberspace area. The GAO is a Congressional office tasked with

providing Congress with findings and recommendations on specific areas of study. The Cyber Efforts report received little fanfare in the media, and portions of it are already dated, but a brief review of the GAO's findings and recommendations provides useful information regarding the internal context within which the DoD has been formulating its policies. The Cyber Efforts report begins by describing the physical size of the problem of protecting DoD digital infrastructure – '7 million computer devices, linked on over 10,000 networks with innumerable satellite gateways and commercial circuits'. The GAO found that this protection task was complicated by a number of significant factors, including the high degree of decentralisation of the efforts to address cyber-security threats among the 'Office of the Secretary of Defense, the Joint Staff, functional and geographic combatant commands, military services, and military agencies'. This problem was further compounded by a lack of clarity in the 'authorities and responsibilities for implementing cyber-operations among combatant commands and military services'. Another area of concern identified in the report was the lack of cohesive and accurate doctrine discussing cyberspace operations. For example, even though at least sixteen DoD joint publications addressed 'cyberspace related topics', none were assessed as adequate. Finally, the report found that although the DoD had 'identified some cyberspace capability gaps, ... it [had] not completed a comprehensive, department-wide assessment of needed resources, capability gaps, and an implementation plan for addressing any gaps'.⁴⁵

The Cyber Efforts report noted that the DoD had agreed with its findings and recommendations, and had launched a number of initiatives to address these problems, including the establishment of US Cyber Command to oversee the DoD cyber-effort. US Cyber Command is co-located with the National Security Agency at Fort Meade, Maryland, and General Keith Alexander is in charge of both DoD organisations. The report concluded, however, that it was too early to tell whether these changes would be effective.⁴⁶ Realistically, given the scope

of the DoD's task to organise itself, establish effective command and control of its cyber-operations, write and validate operating policies and doctrine, recruit and retain cyber-personnel, and acquire equipment, whilst being continuously engaged against numerous potentially hostile actors seeking to get inside its systems, uneven progress in DoD cyber-efforts should not be surprising. Against this backdrop, the lack of substance in the unclassified DoD positions on the applicability and implementation of IHL might be both necessary and adequate at this point in time. From one perspective, uncertainty as to what constitutes a red-line threshold for what the US would consider to be acts analogous to war might cause major state actors to factor this uncertainty into their risk calculations so that they act less boldly than they might have. Conversely, even though risk may not be as important a factor for rogue states and terrorists, uncertainty as to the potential US responses might complicate their planning, and lessen the audacity of any potential attack. The overall effect achieved in cyberspace is then perhaps a reduction of serious attacks, which helps accomplish the overall US strategic goal of a peaceful cyberspace, even if it has not yet exactly figured out how to implement IHL in this context. As Deputy Secretary Lynn acknowledged in his remarks upon the release of the DoD Strategy, however, the current situation in cyberspace is unlikely to be sustained forever. The entire international community has a huge stake in making sure the legal and policy issues regarding the use of force in cyberspace are well understood, and in keeping with accepted norms of international behaviour.

A Way Forward?

Even with the shortfalls in recent and current US organisation and doctrine identified in the Cyber Efforts report, there are a number of programmes underway which should in a holistic and sustainable fashion provide the DoD with the capacity and depth of experience to better flesh out how IHL applies to actions in cyberspace and the practical steps necessary to ensure its proper implementation. By mid-2012,

the DoD expects to have the National Cyber Range operational. This project is intended to be a virtual firing range, and will create a replica Internet within which experimental solutions to cyber-security issues can be tested in fairly rapid succession. The DoD also has an initiative underway to hasten the identification of intruders through the automation of malicious code analysis, dubbed the 'Cyber Genome' project.⁴⁷ If successful, this could lessen some of the legal and policy problems associated with identifying an attacker. Further, the DoD plans to include cyberspace scenarios and cyber 'Red Teams' in training exercises, to give units and personnel the experience of working through situations with degraded cyber-capabilities.⁴⁸ Importantly, not all of the DoD's efforts are geared towards the direct use of force in cyberspace. Under the Defense Industrial Base Cyber Pilot programme, companies that operate networks for the DoD are provided classified threat intelligence which allows them to better protect their systems. The larger goal of the programme is to create a template for military-civilian co-operation that could be used by the DoD in conjunction with other government agencies and areas

of industry such as transportation and energy.⁴⁹

Much of the work that will result from these projects, however, will likely remain classified. Whilst necessary for national security reasons, classification makes the open and critical discussion of IHL's application to situations involving cyberspace much more difficult than discussing the law's application in the physical world. Different nations have different IHL training programmes for their forces, different capabilities, and different domestic legal and policy drivers that govern the way in which the use of armed force is actually applied.⁵⁰ Further, even though they must be consistent with IHL, details of the rules of engagement are classified. However, there is a wealth of experience, study and writing among commentators regarding the use of force in the physical world that allows this discussion to go forward effectively without knowing the precise details. Finally, the means by which force in the geophysical world is employed, both in terms of tactics and equipment, are well understood by many even if they have not been involved in their military use. Conversely, the rapid evolution of cyber-technology and its novel ability to achieve effects akin to those generated by the

use of more traditional forms of armed force would likely make it difficult to describe the practical application of IHL to cyberspace, even if its most important aspects were not classified. The public is therefore unable to determine, for example, whether the DoD's failure to deliver its report to Congress in a timely fashion was the reasonable result of developing such a far-reaching document, or perhaps a signal that the strategy development is flawed or that it had been difficult to achieve sufficient consensus among the stakeholders to go forward at this point. Bridging the gap between the classified cyber communities and the public to foster understanding of which legal norms and policies regarding the use of force are applicable is crucial to ensure transparency and critical assessment of this vitally important area to the greatest extent possible. ■

Jody Prescott is a Senior Fellow, West Point Center for the Rule of Law, and former US Army judge advocate whose career focused on international law, training and education. The opinions expressed in this article are his alone, and do not reflect those of the Center nor the US Military Academy.

NOTES

- 1 Ellen Nakashima, 'Report on "Operation Shady RAT" Identifies Widespread Cyber Spying', *Washington Post*, 2 August 2011.
- 2 US Government Accountability Office, GAO-11-75, 'Defense Department Cyber Efforts: DOD Faces Challenges In Its Cyber Activities', July 2011, p. 1.
- 3 Siobhan Gorman and Stephen Fidler, 'Cyber Attacks Test Pentagon, Allies and Foes', *Wall Street Journal*, 25 September 2010.
- 4 Department of Defense Strategy for Operating in Cyberspace, July 2011, pp. 1-4, <<http://www.defense.gov/news/d20110714cyber.pdf>>, accessed 15 November 2011.
- 5 Nick Hopkins, 'UK Developing Cyber-weapons Programme to Counter Cyber War Threat', *Guardian*, 30 May 2011.
- 6 William J Lynn, 'The Pentagon's Cyberstrategy, One Year Later', *Foreign Affairs*, 28 September 2011.
- 7 Tom Gjelten, 'U.S. Seeks To Define Rules on Cyberwar', *NPR*, 3 June 2010, <<http://npr.org/templates/story/story.php?storyId=127411091>>, accessed 5 August 2011.
- 8 See J P MacIntosh, J Reid and L R Tyler, 'Cyber Doctrine: Towards a Coherent Evolutionary Framework for Learning Resilience', Institute for Security and Resilience Studies, June 2011, <<http://www.ucl.ac.uk/isrs/publications/CyberDoctrine>>, accessed 15 November 2011.
- 9 Rome Statute of the International Criminal Court, Rome, 17 July 1998, art. 8 bis.
- 10 UN Charter, San Francisco, 26 June 1945, art. 41.
- 11 Dieter Fleck, 'Individual and State Responsibility for Intelligence Gathering', *Michigan Journal of International Law* (Vol. 28, 2007), pp. 688-92.
- 12 Use of Force Committee, International Law Association, The Hague Conference, 'Final Report on the Meaning of Armed Conflict in International Law', 2010, pp. 11-13, 28-33.
- 13 *Associated Press*, 'Mexican Troops Involuntarily Cross Into US', 27 July 2011.
- 14 Kirsten Schmalenbach, 'The Right of Self-Defence and The "War on Terrorism" One Year after September 11', *German Law Journal* (Vol. 3, No. 9, September 2002).

- 15 International Court of Justice, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory* (Advisory Opinion) 2004, <<http://www.icj-cij.org/docket/files/131/1681.pdf>>, accessed 4 June 2011 (separate opinion of Judge Higgins, paras. 33, 34).
- 16 John Reed, 'Industry Urges Limits to DoD Cyber Help', *DoDBuzz.com*, 11 February 2011.
- 17 DHS, 'Memorandum of Agreement Between The Department of Homeland Security And The Department of Defense Regarding Cybersecurity', 13 October 2010, <<http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf>>, accessed 7 October 2011.
- 18 Tess Bridgeman, 'The Law of Neutrality and the Conflict with Al Qaeda', *New York University Law Review* (Vol. 85, 2010), p. 1200, note 75.
- 19 Protocol Additional to the Geneva Conventions of 12 August 1949, Geneva, 8 June 1977, art. 51.
- 20 ISAF Public Affairs Office, 'General Petraeus Issues Updated Tactical Directive: Emphasizes "Disciplined Use of Force"', 4 August 2010, <<http://www.isaf.nato.int/article/isaf-releases/general-petraeus-issues-updated-tactical-directive-emphasizes-disciplined-use-of-force.html>>, accessed 5 June 2011.
- 21 The White House, 'International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World', May 2011, p. 5.
- 22 *Associated Press*, 'China Calls US Culprit in Global "Internet War"', 3 June 2011.
- 23 Michele Flournoy and Shawn Brimley, 'The Contested Commons', *DoD Quadrennial Defense Review*, <<http://www.defense.gov/qdr/flournoy-article.htm>>, accessed 7 October 2011.
- 24 International Strategy, *op. cit.*, pp. 5–8.
- 25 *Ibid.*, p. 9.
- 26 *Ibid.*, p. 10.
- 27 *Ibid.*, pp. 12–13.
- 28 *Ibid.*, pp. 11–14. NATO has decided to handle cyber incidents under the consultative procedures of Art. IV of the NATO Treaty rather than as attacks under Art. V. 'NATO Agrees Common Approach to Cyber Defence', *Euractive.com*, 4 April 2008.
- 29 Military Committee, *MC 362/1: NATO Rules of Engagement* (30 June 2003), p. A-1-2.
- 30 While it may not appear possible to use armed force in cyberspace, acts of aggression – defined by international law as 'the use of armed force' – in that sphere may well result in an equivalent effect in terms of the destruction and harm caused, not only to military targets and national infrastructure but also, ultimately, to civilians.
- 31 DoD, 'Department of Defense Strategy for Operating in Cyberspace', July 2010, <<http://www.defense.gov/news/d20110714cyber.pdf>>, pp. 5–12.
- 32 *Ibid.*, p. 7.
- 33 Ellen Nakashima, 'Pentagon Considers Pre-emptive Strikes as Part of Cyber-defense Strategy', *Washington Post*, 28 August 2010.
- 34 William J Lynn, 'Defending a New Domain: the Pentagon's Cyberstrategy', *Foreign Affairs* (September-October 2010), in note 2, pp. 103–04.
- 35 Siobhan Gorman and Julian E Barnes, 'Cyber Combat: Act of War', *Wall Street Journal*, 31 May 2011.
- 36 Letter to Leon Panetta, Secretary of Defense, 20 July 2011, <http://mccain.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=40ca96ab-ec9e-4662-a360-0c1806e44f4e>. Presumably, Senators John McCain and Carl Levin were referring to the War Powers Resolution, which requires that the president inform Congress within forty-eight hours if US forces are engaged in combat, and that Congress authorise continued military engagement in excess of sixty days. See Title 50 of the United States Code, 1541–1548.
- 37 William J Lynn, 'Remarks on the Department of Defense Cyber Strategy', speech made in Washington, DC, 14 July 2011, <<http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1593>>, accessed 5 August 2011.
- 38 DoD Cyber Strategy Report Pursuant to Section 934 of the NDAA of FY 2011, November 2011, pp. 3–4, <http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf>, accessed 16 November 2011.
- 39 *Ibid.*, p. 5.
- 40 *Ibid.*, pp. 6–8
- 41 *Ibid.*
- 42 Gorman, *op. cit.*
- 43 Briefing by DoD General Counsel, 'Joint Targeting Cycle and Collateral Damage Estimation Methodology (CDM)', 10 November 2009, p. 26, <http://www.aclu.org/files/assets/Manes_Declaration_Exhibits.100810.PDF>, accessed 5 June 2011.
- 44 Chairman of the Joint Chiefs of Staff, *Instruction 3121.01B: Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces*, 13 June 2005, p. A3.
- 45 Lynn Remarks, *op. cit.*
- 46 Cyber Efforts report, *op. cit.* pp. 1–8.
- 47 *Ibid.*, pp. 4–6.
- 48 Jim Wolf, 'Pentagon's Advanced Research Arm Tackles Cyberspace', *Reuters*, 16 June 2011.
- 49 DoD Cyber Strategy, *op. cit.*, p. 6.
- 50 Donna Miles, 'Sharing Intelligence Helps Contractors Strengthen Cyber Defenses', *American Forces Press Service*, 16 August 2011, <<http://www.defense.gov/news/newsarticle.aspx?id=65050>>, accessed 7 October 2011.
- 51 Jody Prescott, 'Training in the Law of Armed Conflict: A NATO Perspective', *Journal of Military Ethics* (Vol. 7, No. 1, 2008) pp. 68–72.