Digital Détente:
Designing a Strategic Response to Cyber Espionage

— BY PAUL CORNISH

Cyber Espionage

Cyber espionage – “the use of information technology systems and networks to gather information about an organization or a society that is considered secret or confidential without the permission of the holder of the information”\(^1\) – has been rising steadily to the top of the security policy agenda. Specialist cyber security organisations report a yearly escalation in cyber attacks; the 2011 edition of Symantec’s Internet Security Threat Report, for example, records a 93% increase in the volume of web-based attacks between 2009 and 2010.\(^2\) Also industrial and commercial organizations, which might in the past have been reticent about admitting failure and vulnerability, are now more willing to divulge security breaches. In the words of the director of security research at Trend Micro, “more attacks are being publicly disclosed. Victims are more willing to come forward and say something bad happened to us”.\(^3\)

If the victims of cyber espionage and crime are becoming more willing to divulge their vulnerability, there is also an increasing propensity to “name and shame” the source of these attacks. The turning point is widely supposed to have occurred in 2010 when Google revealed that Chinese hackers, in a campaign known as “Operation Aurora,” had penetrated it. But that move had been anticipated some months earlier by
Richard Clarke, a former special adviser on cyber security to U.S. President George W. Bush, and someone known for his bleak assessment of the cyber security challenge. “Information technology experts in and out of government” wrote Clarke in May 2009, “believe that American corporations are regularly losing to foreign cyber espionage (most likely China’s) what gives U.S. firms their competitive edge: the results of expense on R&D, engineering plans, chemical and biological formulas, complex software, even customer lists and pricing data.”

Private sector concerns about Chinese cyber espionage reached a crescendo in spring and summer 2011. The British industrialist James Dyson warned that “Chinese students are infiltrating British universities to steal technological and scientific secrets and even planting software bugs to relay the information to China. I’ve seen frightening examples. Bugs are even left in computers so that the information continues to be transmitted after the researchers have returned home.” The Chinese embassy in London refuted Dyson’s claim as “shocking and entirely unfounded and illogical” and a “damaging slander to all Chinese students.” But McAfee, another cyber security organization, then accused a single “state actor” of a long-running series of cyber attacks against an unusually wide variety of more than seventy organisations including the United Nations, the Association of Southeast Asian Nations and various defence contractors. Although McAfee did not name China as the culprit, “independent security experts” were reported to believe that “Beijing was the most likely culprit.”

As well as a distinct sharpening of attitudes within the private sector, there is also mounting evidence that the public policy establishment is becoming less reticent about identifying the sources of cyber espionage. In June 2009 an article in the New York Times reported the concern of unnamed “United States officials” in the recently formed Obama administration that “a significant proportion of the attacks against American government targets are coming from China and Russia.” Similarly, in the UK the Secretary of State for Defence warned in June 2011 that the Ministry of Defence faced “cyber-war attacks on a daily basis” and that “our national intellectual property in defence and security industries is at risk from systematic marauding” originating in China.

The UK Security Service was reported, also in June 2011, to have accused China of devoting “considerable time and energy trying to steal our sensitive technology on civilian and military projects and trying to obtain political and economic intelligence at our expense.” And in October 2011 the head of cyber security in the UK Ministry of Defence warned that “The biggest threat to this country by cyber is not military, it is economic.” Claiming that “the Chinese pose the biggest threat” the official went on to observe: “If the moment you come up with a brilliant new idea, it gets nicked by the Chinese then you can end up with your company going bust.” Both the style and the substance of this comment were reprised some weeks later when Mike Rogers, the Republican chairman of the U.S. House of Representatives Permanent Select Committee on Intelligence, claimed that Chinese hackers and spies “are stealing everything that isn’t bolted down, and it’s getting exponentially worse.” Just months earlier, the U.S. Office of the Director of National Intelligence (DNI) had published a report which asserted, with undiplomatic frankness that “the computer networks of a broad array of U.S. government agencies, private companies, universities, and other institutions – all holding large volumes of sensitive economic information – were targeted by cyber espionage; much of this activity appears to have originated in China.”

The rhetoric has been escalating steadily to the point that an international confrontation is becoming conceivable, with all the disruption and harm that might entail. Given the value placed on digital communications this is scarcely a comfortable prospect. It is legitimate therefore to ask what should be done, if not to resolve that confrontation then at least to manage it as it becomes more entrenched.

For some, the Cold War can provide useful lessons in crisis management among adversaries and there is a growing interest in extending Cold War strategic thought – particularly deterrence – into cyber space. But it is at this point that things become complicated. For all the discussion of cyber espionage it remains in policy terms curiously primitive, as if its development has been arrested in a pre-strategic condition: it is not easily located on the security policy/strategic spectrum; it is notoriously difficult to attribute; and the tools with which it might be managed are not readily identifiable.

If Cold War strategic thought is to contribute to the cyber espionage debate it will require some modification. The aim should be to move cyber espionage from non-communicative adolescence into something like a mature strategic relationship, which can then be stabilised and improved. The “attribution problem,” discussed below, is the greatest impediment to this shift. In cyber space generally, and particularly in the field of cyber espionage, the most prized assets are anonymity, deniability and uncertainty and it is hard to imagine a strategic relationship developing under such conditions. An imaginative application of deterrence thinking can, however, move the cyber espionage debate in the right direction, creating a strategic relationship, which can then be managed, in the digital equivalent of détente.

For all the discussion of cyber espionage it remains, in policy terms, curiously primitive — as if its development has been arrested in a pre-strategic condition.
The Attribution Problem

In its various guises, the cyber security debate is bedevilled by the problem of attribution: the difficulty (some would say impossibility) of establishing with sufficient confidence the identity and location of an attacker. This in turn makes it difficult to penetrate the “plausible deniability” defence behind which any cyber aggressor (cyberspy, cyber-terrorist, cyber-criminal and perhaps even a “cyber-warrior”) can hide. Discussion of Chinese cyber espionage provides a good illustration of the problem.

In broad terms there are three contending perspectives on the question of Chinese cyber espionage. The first, which could hardly be more alarming, was offered at a conference organized by the Jamestown Foundation in Washington in February 2011. Here, the Chinese were described as “seeing digital attacks differently than U.S. planners.” China would play a “long game” in which they would, essentially, prepare the battlefield for a subsequent, more traditional conflict by ensuring that U.S. supply and logistic chains could be degraded at the critical moment. In order to infiltrate core networks, China would allow exported hardware to be inspected for security but would then “introduce malicious software via upgrades, maintenance, and other post-buy actions.” Others have similar suspicions. A report published in late 2010 by the Economist newspaper wondered whether “cyber weapons” could serve as “an assassin’s mace” in a surprise attack designed to smash America’s elaborate but fragile electronic networks. That would leave American forces half-blind and mute, and its bases and [aircraft] carriers more vulnerable still.14

The second perspective is altogether more skeptical. The answer to the question “Why should China be involved in cyber espionage?” might begin with two observations: first, as is widely acknowledged, the barriers to entering the world of cyber espionage are relatively low; and second, as is also generally accepted, China has very high levels of high quality human capital in information and communications technology. If China has indeed become one of the world’s most active practitioners of cyber espionage, rather than ask why this is taking place the better question might be “Why should China not be undertaking widespread cyber espionage?” Cyber espionage could be considered an entirely rational activity, insofar as it confers so-called “asymmetric” advantages for a growing economy and offers a level of insurance against an uncertain and undecided future. By this view, Chinese cyber espionage might be much less than the early warning of an impending global confrontation. China might, instead, be doing what any other state would do in similar circumstances – exploiting what it perceives to be a passing strength until its adversaries, competitors and partners improve their performance and the “playing field” of international cyber security and commerce is levelled. As Joseph Nye has observed, “in the area of industrial espionage, China has had few incentives to restrict its behaviour because the benefits far exceed the costs.”15
The third perspective is that Chinese cyber espionage is little more than an alarmist concoction of the West’s own making, designed to privilege certain departments or agencies of government over others or to make the case for government spending on this or that equipment or capability; a digital-age reprise, perhaps, of the “military-industrial complex” of the early Cold War.

By one view, fears of Chinese cyber expertise are wildly exaggerated, with China more accurately ranked “near the bottom of the table” of comparative national cyber power. As Amitai Etzioni has observed, there is always the risk that the persistent description of China as a sophisticated cyber-adversary will at some point become a self-fulfilling prophecy.¹⁸

For as long as accurate attribution is considered to be both critical to the policy debate yet at the same time largely unattainable, it is difficult to decide which of these three perspectives is the most reasonable. The attribution problem makes it hard to judge with enough confidence whether or not China is involved in cyber espionage and, if so, what its motives might be. It is for this reason that I describe the cyber espionage debate as being in a state of arrested development, held at the level of speculation rather than strategy. The consequences of this are more than merely analytical, however. While cyber espionage remains under-developed and opaque as a strategic problem, it also remains impervious to careful management. And so it becomes ever more difficult to develop a co-operative relationship with cyber adversaries and competitors, rather than a relationship which might be either unnecessarily confrontational or unwisely complacent.

Deterrence and Détente

The Cold War showed how mutual deterrence could stabilize a confrontational strategic relationship.¹⁹ Without that stability it would not have been possible for détente, the more progressive idea, to gain any purchase. Cold War deterrence came in two models. The first, “deterrence by punishment,” functioned by threatening such a devastating response to any nuclear attack that the potential attacker would be persuaded not to proceed. Punitive deterrence of cyber espionage is less straightforward, however. Asymmetric deterrence – i.e. nuclear deterrence of a non-nuclear attack, or military deterrence of a non-military incursion – was always a complicated proposition. And given the attribution problem it is even more difficult to imagine that a large-scale military response would be made in the face of an opaque cyber attack of some sort. Nevertheless, the idea is never entirely discounted; the United States, for example, is reported to have come to the conclusion that “computer sabotage coming from another country can constitute an act of war, a finding that for the first time opens the door for the United States to respond using traditional military force.”²⁰

The second model, “deterrence by denial”, sought to influence an adversary’s decision calculus in a less direct manner by showing that defensive preparations would make the costs of mounting a successful attack so high as to outweigh any benefits. Here, the relevance to cyber espionage is more obvious; governments and the private sector already take defensive and preventive measures to protect their cyber capabilities. Sometimes described as “active cyber defence,”²¹ these measures could range from improved and more open working between the public and private sector to make the information infrastructure more resilient (given that most of the infrastructure upon which government and national security, and indeed the national economy depend is privately owned),²² to the continued development of Computer Emergency Response Teams at the national and multilateral level.²³ Measures such as these, together with improved network and data security and other physical and personnel security measures, could all affect a potential cyber-adversary’s assessment of risk and reward. In other words, these measures would make clear that the target state or organization is not only aware that it is the victim of espionage but is also taking measures to make it less likely that espionage will succeed, or that a far greater investment will be required if it is to do so.

Cold War deterrence – by the threat of punishment and by denial – stabilized the strategic confrontation and made it fit for détente. Détente was an attempt by Cold War protagonists to reintroduce trust in a confrontational strategic relationship which, during the 1960s and 1970s, was becoming ever more strained and prone to miscalculation, with the prospect of devastating results. Détente did not survive much beyond 1980, but at its core was a simple yet compelling idea which has not disappeared from strategic memory. To an important extent, what motivated détente was a view of the world as a commons, severe damage to which would be felt generally. By the 1960s, the nuclear arsenals of the United States and the Soviet Union were increasingly being designed to ensure that neither side would lose in a nuclear exchange. The claim of détente, conversely, was that widespread and severe devastation resulting from a nuclear war would mean that neither side could be said to have won.

It is at this point that the analogy between cyber espionage and the Cold War becomes rather stretched. During the Cold War it could not reasonably be denied that the East-West confrontation existed ideologically, politically and militarily, and there was an urgency to managing and resolving that confrontation. But these things cannot of course be said of a non-attributable cyber confrontation. In one respect, however, the Cold War analogy remains useful; the notion of a vulnerable commons, the protection of which will be to mutual benefit.
The claim that cyber space can be understood as a “global technological commons” can elicit an allergic response in some analysts who point out that unlike oxygen, rain, the wind and the high seas, cyber space is not a naturally occurring phenomenon. Cyber space is instead a system of machines which are built, owned and maintained by people – Andrew Blum writes compellingly of the “physical infrastructure” of the Internet. Yet what is striking about cyber space – and relevant for this article – is that its users behave as though it were indeed a benefit in common; for most users, the technology has become indispensable while the cost has been driven down to the marginal. As a result, in commercial jargon the “users” and “customers” of cyber space have come to see themselves as “stakeholders” and even “guardians” of a facility to which they have a right. “Earthrise,” the first image of the earth taken from space in December 1968 stimulated the growth of the environmental movement and added to the pressure for strategic détente. The digital-age equivalent of that moment is the perception that the global communications and commercial infrastructure is owned in common and must be protected. It is this idea which should motivate strategic thought in the digital era. Whereas Cold War détente was concerned in part to prevent the destruction of the highly valued physical commons, digital détente should be concerned to prevent the breakdown of the global technological commons. Two versions of deterrence can bring cyber espionage closer to this point: “deterrence by interdependence” and “deterrence by association.” Both constitute a norm-building exercise for cyber space around which a stable strategic relationship can be built. Once built, that relationship can be amenable to a digital equivalent of détente.

Deterrence by interdependence begins from the commonplace argument that national interests are best secured through the shared pursuit of an open, fair and regulated cyber space. Most national economies are irreversibly inter-connected in the global economic system and it is therefore in the interest of those states that there should be a functioning global economy with international trading partners, as well as a reliable international information and communications infrastructure.

It follows that states should be wary of cyber espionage and similar activities which might be costly and which might damage the global digital economy and themselves in the process. A state which undertook cyber espionage would not only have to be technologically proficient so as to escape detection, it would also have to be sufficiently robust so as to manage the economic shocks and turbulence that would result. There is also the question of economic resilience to consider. Although the theft of intellectual property might appear to compensate for certain disadvantages in the short term, as Adam Segal has observed it must be difficult to build and maintain a genuinely innovative and dynamic economy “when you’re busy stealing intellectual property.”

If deterrence by interdependence prefers certain behaviours and prohibits others, deterrence by association takes the norm-building exercise to the next level by emphasising the diplomatic, political and reputational damage that can result from being seen to tolerate, support or gain from pariah behaviours. This is neither a novel nor a complex idea, and is already at work in the field of nuclear proliferation: “if states and commercial organisations can be exposed for having supplied a nuclear weapon capability to a terrorist group, they can then be subject to sanctions; and the threat of sanctions might have the effect of cutting off supply in the first place.” For deterrence by association to work, a number of steps must be taken. Public and private sector organisations which have been the victim of cyber espionage must be more forthcoming about the incidence of cyber espionage attacks and, particularly, about the level of harm caused. The victims should also be willing to discuss, in public, their best estimates of the origin of a cyber espionage attack, who or what might have orchestrated it and who might have gained from it. The purpose of the exercise would be to re-engineer the cyber espionage debate in a subtle way, by developing the norm that association with such behaviours would be reputationally damaging and should therefore be avoided. As the norm becomes more established so the onus would be placed on governments to demonstrate that they were not involved, as sponsors or beneficiaries, in cyber espionage or in any given event, rather than to argue that their involvement cannot be proved. The attribution problem will remain, certainly. But the core argument of deterrence by association (not “deterrence by proof”) is that a political, rather than a technological standard
of evidence can and should be used and that governments and the private sector should be encouraged not just to form judgements but to discuss them more openly as encroachments on the commons.

**Conclusion**

In his analysis of cyber relations with China, Amitai Etzioni assesses the relative merits of the “adversarians” against the “engagers.” “The first group” observes Etzioni, “tends to consider the rise of China as threatening to the United States interests and the world order.” The “engagers” on the other hand, tend “to consider China as a nation that seeks to focus on its own development and can be engaged to work with the United States and other nations to advance shared interests and the common good.”

Etzioni’s operating assumption, clearly, is that there is a strategic relationship with China which is susceptible to management in one direction or the other. The contention of this article, however, is that strategic relationships must first be made before they can be stabilised and improved. Yet at present, and as a consequence of the attribution problem, relationships between cyber adversaries and competitors are at best pre-strategic; held in a state of arrested development.

Strategic thought, from the Cold War and earlier, can be useful in addressing cyber security challenges – including cyber espionage – but only if applied with imagination and with some modification. In a curiously circular way, at this early stage in the development of cyber security as a strategic problem, the purpose of strategy should be to make strategy possible. The goal should be for cyber espionage to become a subject for serious, balanced public policy discourse and for cyber space itself to become a strategic arena in which diplomacy, negotiation, bargaining, compromise and concession can all have their place. In its various forms, deterrence can assist in this process. Deterrence can be both protective and defensive, as well as constructive of a more sophisticated and progressive relationship with an adversary or competitor.

Deterrence by association falls into the latter category. By emphasising the most distinctive features of cyber space – that it has acquired universal value; that access to it is increasingly seen as a right; and that it is being encroached upon – deterrence by association offers the normative point of reference which has so far been lacking in the cyber strategy debate, largely a result of the impasse caused by the attribution problem. Deterrence by association is a high risk strategy, politically and diplomatically, but it can establish the ground rules of a strategic relationship which can then develop into a policy of containment, if necessary, or engagement if possible through the digital equivalent of détente.

Professor Paul Cornish is Professor of International Security at the University of Bath. He was educated at the University of St Andrews (modern history), the London School of Economics (international relations) and received his Ph.D. from the University of Cambridge. He is a member of the UK Chief of the Defense Staff’s Strategic Advisory Panel, and has contributed to a number of Parliamentary inquiries and is a frequent commentator in national and international media.

---

**REFERENCES AND NOTES**


REFERENCES AND NOTES


19 This section is drawn from P. Cornish, Chinese Cyber Espionage: Confrontation or Co-operation? (Bath: Cityforum Ltd, April 2012): https://www.cityforum.co.uk/publications.asp


21 “Active cyber defence” is defined by the U.S. Department of Defense as synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities”: Department of Defense Strategy for Operating in Cyberspace (Washington, D.C., July 2011), p.7.


26 “Commons” is defined in the Oxford English Dictionary as “provisions for a community or company in common”.

