Journal of Strategic Studies
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/fjss20

Cyber War Will Take Place!

John Stone [a]
[a] Department of War Studies, King's College, London, UK

Version of record first published: 29 Nov 2012.

To cite this article: John Stone (2013): Cyber War Will Take Place!, Journal of Strategic Studies, 36:1, 101-108

To link to this article: http://dx.doi.org/10.1080/01402390.2012.730485

The Journal of Strategic Studies, 2013
Vol. 36, No. 1, 101–108, http://dx.doi.org/10.1080/01402390.2012.730485

Cyber War *Will* Take Place!

JOHN STONE

Department of War Studies, King's College London, UK

ABSTRACT The question of whether or not cyber war amounts to war *per se* is difficult to determine given strategic theory's uncertain grasp of the concepts of force, violence and lethality. These three concepts, along with their relationships with one another, are explored in order to demonstrate that cyber attacks can in fact be construed as acts of war.

KEY WORDS: Cyberwar, Force, Violence, Lethality, Strategic Theory

Cyber war will take place! Well perhaps not, but my purpose here is to demonstrate that cyber war *could* take place – despite some lively and imaginative arguments to the contrary.

One of the most interesting things about the burgeoning debate on cyber war is the ready manner in which it exposes our precarious grasp of the concepts we routinely employ in our discourse about war as such. Efforts to determine whether cyber attacks should be considered acts of war, or whether they are better understood as criminality, espionage, or sabotage etc., are hampered by our loose understanding of what war itself amounts to. More specifically the means of war, whether construed as force or violence, remain under-explored and under-specified by strategic theorists. As a result, these terms are typically used both loosely and interchangeably, undermining their value as conceptual tools in the process.

Perhaps the most important reason for this enduring lack of conceptual precision is bound up with the historical development of Strategic Studies. Strategy emerged as an intellectual field of endeavour in response to the invention of nuclear weapons. The overriding goal was to identify ways of ensuring that another great-power war would never again happen. Under these circumstances, strategic theory acquired a pragmatic character: the emphasis was on providing workable solutions to pressing problems of policy. As Bernard Brodie

noted during the Cold War, the 'question that matters in strategy is: Will the idea work?'[1] Consequently, strategists were never particularly concerned with the fundamentals of war, violence and force; their focus was always on the specifics of nuclear weapons and on strategies of deterrence. Although this situation was recognized by some at the time, a more fundamental engagement with the phenomenon of war was not forthcoming. When, in a somewhat different context, Hannah Arendt decried the lack of precision with which 'such key words as ''power'', ''strength'', ''force'', ''authority'', and, finally, ''violence'' – all of which refer to distinct, different phenomena' were employed, strategic theory had nothing to offer by way of clarification.[2]

This remained the case until the end of the Cold War, at which point nuclear deterrence became a less pressing matter, there being comparatively little left to deter. Any notion that strategists might now be able to draw breath, and embark on a more fundamental engagement with the phenomenon of war, proved erroneous, however. This was because the intellectual climate of the immediate post-Cold War years militated against any such development. The tendency was not so much to engage with the fundamentals of war, as to relegate Strategic Studies to a liminal position within the much broader framework of Security Studies.[3] Whatever war might be, it was increasingly considered just one among many threats to the common weal, and not the most urgent one at that. Thus when war once again became a serious policy issue – initially in the guise of ethnic conflict, and subsequently of international terrorism and insurgency – a firm grasp of fundamental matters was still not evident. The tendency was to treat each new manifestation of war as something sui generis, rather than some variation on a common phenomenon. If anything this tendency worked to fracture the concept of war as a distinct form of political activity, and to replace it with a disparate series of undertakings distinguished by their particular modes of strategic action. War became 'humanitarian intervention' and 'counter-insurgency'.

It is, therefore, hardly surprising that the question of whether or not something as unconventional as cyber attacks constitute an act of war is a contentious one. In the absence of a clear basis for understanding what *any* act of war amounts to, we are unlikely to be able to reach

[1]Bernard Brodie, *War and Politics* (London: Cassell 1973), 452.

[2]Hannah Arendt, *Crises of the Republic* (Harmondsworth, UK: Penguin 1973), 112. As Arendt noted (p. 87, n. 6): 'There exists, of course, a large literature on war and warfare, but it deals with the implements of violence, not with violence as such.'

[3]For a discussion of the relationship between Strategic Studies and Security Studies in the immediate wake of the Cold War see R.K. Betts, 'Should Strategic Studies Survive?', *World Politics* 50 (1997), 7–33.

agreement on the status of cyber attacks. More specifically, the allegedly 'bloodless' character of cyber attacks is particularly challenging, because it demands that we think through the relationships between force, violence and lethality more systematically than has hitherto been done. In what follows, I propose to illustrate these points in relation to a single, particularly influential, article by Thomas Rid that was published in a recent issue of *The Journal of Strategic Studies*. Rid's principal argument is that there is no such thing as cyber war today, and nor will there be so in the future. 'Cyber War', he contends, 'Will Not Take Place.'[4] This, he maintains, is because no instance of cyber attack to date has embodied all those necessary features that comprise an act of war – and nor, by implication, are such attacks likely to do so in the future. Cyber attacks may be auxiliary to an act of war, but they do not constitute such an act in and of themselves.

So what, exactly, is an act of war? According to Rid, any act of war must embody three particular features: it must be political in motivation, instrumental in character and lethal in potential. The first two of these features are unremarkable enough: they are merely a reformulation of the Clausewitzian position on war's political instrumentality. We shall return a little later to Rid's particular view of what constitutes a political act, and the importance he attaches to attribution in this context. For the present, I want to focus in some detail on the matter of lethality and its relationships with force and violence. Rid's understanding of these relationships is set out most clearly and concisely in the following passage:

> 'War is an act of force to compel our enemy to do our will', wrote Carl von Clausewitz on the first page of *On War*. All war, pretty simply, is violent. If an act is not potentially violent, it is not an act of war ... A real act of war is always potentially or actually lethal, at least for some participants on at least one side.[5]

This passage is particularly interesting because here we find Rid conflating force, violence and lethality in something like the manner that so exercised Arendt: force implies violence, which in turn implies lethality. In fact, however, war demands no necessary causal connection between what are really three distinct phenomena. As we shall see next, all war involves force, but force does not necessarily imply violence – particularly if violence implies lethality.

[4]T. Rid, 'Cyber War Will Not Take Place', *Journal of Strategic Studies* 35/1 (Feb. 2012), 5–32.
[5]Ibid., 7.

As Rid rightly notes, Clausewitz characterizes war as 'an act of force' (*ein Akt der Gewalt*). The word *Gewalt* can, of course, mean both violence and force (not to mention power and control). But Clausewitz is concerned to be specific. When he describes *Gewalt* as the means of war, he is thinking in terms of physical force (*die physische Gewalt*).[6] He is, in other words, referring to the kind of force that enjoys a formal scientific meaning associated with the capacity to cause physical change. We can be confident that Clausewitz had this form of usage in mind; his work is, after all, rich in analogies with classical physics, of which the best known is 'friction'. In physics the term 'friction' denotes surface resistance to movement. As such it evidently recommended itself to Clausewitz as a label for the multitude of influences that conspire to ensure that no army ever operates with perfect efficiency.

How does force achieve effects in war? One way it does so is by imposing physical change directly on human bodies, injuring or killing in the process. In this context, force is applied in a manner calculated to produce effects that we routinely label as 'violence' in our everyday discourse. The *Oxford English Dictionary* (*OED*) defines violence as 'behaviour involving physical force intended to hurt, damage, or kill'. On this reading of matters, force is violative of human bodies and may prove lethal in consequence. Dead soldiers are the result, and these deaths reduce a belligerent's capacity for imposing his will on an adversary. Here, therefore, force, violence and lethality combine to produce Rid's third defining condition for an act of war. Matters do not end there, however, because to allow that acts of war always involve force and violence is not to allow that they must involve lethality (or injury). As far as the *OED* is concerned, it would seem that force can be violative of more than just human bodies. The term 'damage' implies that violence may be directed at artefacts as well as people, which means that it need not always be lethal in nature. This, moreover, is a reading of the situation that is amply supported by the historical record.

In 1943 the US 8th Army Air Force conducted two raids over the Bavarian town of Schweinfurt. In both cases the intention was to cripple German ball-bearing production, almost all of which was centred on the town. In the first raid 203 people were killed on the ground, in the second 276.[7] As far as the Allies were concerned, these deaths were incidental to the desired goal of destroying the enemy's capacity for manufacturing ball-bearings. The factories were the real target: destroy them and German war production would be critically

[6]Carl von Clausewitz, *Vom Kriege*, 19th ed. (Bonn: Ferd. Dümmler 1989), 191–2.
[7]Thomas M. Coffey, *Decision Over Schweinfurt: The US 8th Air Force Battle for Daylight Bombing* (London: Robert Hale 1978), 60, 325.

compromised. To this end the raids involved daylight precision bombing against relatively small targets, and the level of accuracy achieved was impressive by the standards of the day. Ball-bearing production was seriously curtailed and Germany's minister for war production, Albert Speer, concluded that further raids of this kind would have had fatal consequences for the war effort as a whole.[8] That the 8th Air Force did not subsequently return to Schweinfurt was due to the number of bombers and crews it lost in the process of mounting long-range daylight raids in the face of capable air defences.

This example is revealing for what it suggests about the relationship between violence and lethality – which is that the two are not inexorably linked. The casualties suffered on the ground were an unintended (if foreseen) consequence of the raids: they were not the desired end of the bombing. To insist on a lethal dimension to violence would, therefore, be to deny the Schweinfurt raids the status of acts of war. We should have to call them something else. More than this, it would require a new term for the characteristically Western liberal way of war that, since Liddell Hart, has been predicated on minimizing loss of human life by employing advanced military technique to strike rapidly and accurately at the material components of the enemy's means of resistance. The Schweinfurt raids were but one early example of such long-running efforts, which have more recently been pursued under the guise of the 'Revolution in Military Affairs' and the Pentagon's 'Military Transformation' initiative.

Rid prefers the term 'sabotage' for any 'deliberate attempt to weaken or destroy an economic or military system' where '*things are the prime targets, not humans*'.[9] From this perspective, the Schweinfurt raids, along with the Liberal way of war in general, could indeed be viewed as grand attempts at sabotage – but this does not prevent them from also being acts of war. The two are not mutually exclusive. This may be why Rid also stipulates that sabotage eschews 'open violence' and 'political attribution', while war always involves them. 'Any violent act and its larger political intention' he claims, 'has to be attributed to one side at some point during the confrontation. History does not know acts of war without eventual attribution.'[10] But (even if it is true) this historical claim does not exclude the possibility that future war *could* involve unattributed acts of force, producing violence and possibly lethality along the way. Clausewitz's definition of war as an act of force does not require that the act be claimed or attributable. Strategic actors might

[8]Albert Speer, *Inside the Third Reich*, tr. Richard and Clara Wilson (London: Weidenfeld 1970), 285.
[9]Rid, 'Cyber War Will Not Take Place', 16, with original emphasis.
[10]Ibid., 8, 16.

conceivably harbour carefully concealed political goals that they seek to achieve via covert acts of force. In short, matters of openness and attribution are not germane to any attempt at distinguishing between war and sabotage. In the end, therefore, Rid's distinction between war and sabotage rests solely on matters of targeting: war involves killing people, sabotage involves breaking things; war involves lethality, sabotage does not. But, as we have already noted, maintaining a distinction on this basis would necessitate re-describing the whole liberal way of war – which has principally been concerned with breaking things as an alternative to killing people – as sabotage. This is not a realistic move, not least because it involves doing too much violence (*sic*) to accepted notions of what amounts to an act of war. And, because it is not a realistic move, we are amply justified in concluding that war need not involve the generation of lethal violence. At this point, therefore, lethality drops out of the picture. Acts of war do not require its presence and nor, moreover, can the status of cyber attacks be judged on this basis.

There is, however, a second possible objection (this one not entertained by Rid) to the claim that cyber attacks constitute acts of war. This objection rests not on the relationship between violence and lethality, but on the relationship between force and violence. As previously mentioned, Clausewitz defined war as an act of physical force rather than of violence. In this context, violence must be considered a product of force rather than a defining feature of war. This might seem to undermine the warlike status of cyber attacks because they do not appear to rely on force as their efficient mechanism. Violence aplenty might well stem from a cyber attack, but would this be the result of an act of force? The situation we are presented with here is reminiscent of the borderline cases that philosophical investigation into the relationship between force and violence routinely throws up. C.A.J. Coady provides two such vexing instances in this regard: 'One example is a stabbing to death with a stiletto gently slid between the ribs … a second example (or class of examples) concerns poisoning or gassing.'[11] Cyber attacks would seem to fit rather neatly into this category of problematic cases where violence appears to be rather more in evidence than does force.

One way of tidying up many of these borderline cases is to consider them not simply as questionable acts of force, but as acts of force whose outcomes are augmented by technology. In the context of war, technology is often described as a 'force multiplier', although for present purposes it is better termed a 'violence multiplier'.[12]

[11]C.A.J. Coady, 'The Idea of Violence', *Journal of Applied Philosophy* 3/1 (1986), 16.
[12]For an example of technology being considered as a force multiplier see J. Stone, 'Technology and War: A Trinitarian Analysis', *Defense and Security Analysis* 23 (March 2007), 27–40.

Technology, in other words, constitutes a medium of action through which the application of small amounts of force are translated into large amounts of violence. The 'stiletto gently slid between the ribs' provides one such example. A stiletto is a form of dagger specially adapted for use as a stabbing weapon. As such it is characterized by a thin blade tipped with a sharp point. The point of the point (so to speak) is to focus the physical force generated by an act of stabbing onto a very small area, thus facilitating a deep wound of the kind necessary to damage internal organs. The stiletto, in other words, is carefully designed to maximize the violence stemming from it being 'gently slid between the ribs'. Much the same can be said for cases of poisoning or gassing. Here poisons or gas work to augment the level of violence beyond that which might otherwise be produced by the act of force associated with delivering them to their target. Poison darts can thus produce deadly pinpricks, while gas shells can produce lethal effects far downwind of their point of detonation.[13] On this basis, cyber attacks represent a particularly efficient means of translating force into violence: a few key strokes are all that are required to set in train a sequence of potentially very violent events.

In conclusion, cyber war is possible in the sense that cyber attacks *could* constitute acts of war. This point only becomes evident, however, if we are clear about what is encompassed by the terms 'force' and 'violence', and about their relationship with the matter of lethality. Acts of war involve the application of force in order to produce violent effects. These violent effects need not be lethal in character: they can break things, rather than kill people, and still fall under the rubric of war. Moreover, the mediating influence of technology means that small acts of force – such as tapping a keyboard – can result in large amounts of violence, lethal or otherwise. None of this is to belittle Rid's stimulating efforts. The value of his argument rests not so much on whether it is right or wrong, but on its capacity for provoking debate about cyber war and, by extension, about the fundamentals of war itself. The fact that we lack a substantially agreed upon conceptual framework within which to locate cyber attacks is not the fault of any single individual but of the field of Strategic Studies as a whole. Rid has done the great service of holding up a mirror to those of us who work in this field, and inviting us to think about what we see in it.

[13]Another of Coady's cases – that of slow-acting poison requiring the administration of several doses – is difficult to fit into this framework, but nor is it something that one might routinely wish to characterize as an act of war.

Note on Contributor

John Stone is a Senior Lecturer in the Department of War Studies, King's College London, where he specializes in the history and theory of military strategy. His latest book is *Military Strategy: The Politics and Technique of War* (London: Continuum 2011).

Bibliography

Arendt, Hannah, *Crises of the Republic* (Harmondsworth, UK: Penguin 1973).
Betts, R.K., 'Should Strategic Studies Survive?', *World Politics* 50/1 (Oct. 1997), 7–33.
Brodie, Bernard, *War and Politics* (London: Cassell 1973).
Clausewitz, Carl von, *Vom Kriege,* 19th ed. (Bonn: Ferd. Dümmler 1989).
Coady, C.A.J., 'The Idea of Violence', *Journal of Applied Philosophy* 3/1 (1986), 3–19.
Coffey, Thomas M., *Decision Over Schweinfurt: The US Army Air Force Battle for Daylight Bombing* (London: Robert Hale 1978).
Rid, T., 'Cyber War Will Not Take Place', *Journal of Strategic Studies* 35/1 (Feb. 2012), 5–32.
Speer, Albert, *Inside the Third Reich*, tr. Richard and Clara Winston (London: Weidenfeld 1970).
Stone, J., 'Technology and War: A Trinitarian Analysis', *Defence and Security Studies* 23 (March 2007), 27–40.