The Journal of Strategic Studies, 2013
Vol. 36, No. 1, 139–142, http://dx.doi.org/10.1080/01402390.2012.742012

More Attacks, Less Violence

THOMAS RID

King's College London, UK

ABSTRACT A response to John Stone, Dale Peterson, and Gary McGraw on cyber war.

KEY WORDS: Cyber War, Cyber Security, Violence, Sabotage, Power

The discussion of cyber war, indeed the discussion of war, is hampered by a lack of precision. That lack of precision is widespread, as John Stone pointed out in his powerful critique of my original article. This confusion may be bound up with the history of the discipline of strategic studies and its unwieldy Cold War-baggage. Stone's criticism is two-pronged: he maintains that I did not properly distinguish violence, force, and power, merged in the German *Gewalt*; and second he argued that my distinction between war and sabotage would 'do too much violence (sic) to accepted notions of what amounts to an act of war'. I consider both arguments in turn.[1]

Violence

Violence administered through cyber attack differs from traditional violence in several ways. Two stand out: violence inflicted through computer code is *indirect* and *unqualified*. First, the human body is not directly vulnerable to cyber attack, only indirectly. The reason for this is as banal as it is important: computer code, on its own, cannot harm a biological system, only a computer-controlled technical system. A cyber attacker with violent ambitions has to 'weaponise' a primary target system. Any cyber attack with the goal of physical destruction, be it

[1]John Stone, 'Cyber War *Will* Take Place!,' *Journal of Strategic Studies* 36/1 (February 2013), <http://dx.doi.org/10.1080/01402390.2012.730485>. See also Thomas Rid, 'Cyber War Will Not Take Place,' *Journal of Strategic Studies* 35/1 (February 2012), 5–32.

material destruction or harming human life, has to utilize force or energy that is embedded in that targeted system or created by it. Code, quite simply, does not come with its own explosive charge. Code-caused destruction is therefore *parasitic on a target*. And that primary target cannot be a human body. Yet the human body, in several ways, is the foundation of violence.

This leads to the second observation: that indirect code-borne violence is bound to remain unqualified. To understand this, it is indeed necessary to take up Stone's recommendation, to go beyond strategy, and seek help in political theory. Taking the human body as the starting point for political theory has a long tradition, especially among political philosophers concerned with the phenomenon of violence and how to overcome it.[2] A most powerful driving force for all political organization is the universal weakness of all humans, and their resulting need for political organization to abolish the use of violence for self-help and overcome a natural state of conflict. One of the most inspiring writers on this subject is Alessandro Passerin d'Entrèves, a mid-twentieth century political philosopher who strongly influenced Hannah Arendt's writings on violence, quoted by Stone. In *The Notion of the State*, Passerin d'Entrèves discusses the use of force at length. The political thinker was struggling with the age-old question for, as he called it, the long and mysterious ascent that leads from force to authority, what transforms 'force into law, fear into respect, coercion into consent – necessity into liberty'.[3] Force, when used by the sovereign in order to enforce the law, ceases to be mere violence. By representing the legal order, force becomes institutionalized, 'qualified' in Passerin d'Entrèves's phrase, 'force, by the very fact of being qualified, ceases to be force' and is being transformed into power.[4] Violence administered through computer code, as a result of its indirect nature, is bound to remain unqualified. The German language, remarkably, never disqualified violence. The notion of *Cybergewalt*, or indeed cyberpower, makes little sense – not pointing out this crucial limitation is a shortcoming of my original article, not its narrow conception of violence.

[2]See the opening paragraph of chapter 13, 'Of the naturall condition of mankind, as concerning the felicity, and misery', Thomas Hobbes, *Leviathan* (London: Penguin 1996 [1651]), 86.

[3]Alessandro Passerin d'Entrèves, *The Notion of the State* (Oxford: Oxford University Press 1967), 2.

[4]See Hannah Arendt's discussion of Passerin d'Entrèves's contribution, Hannah Arendt, *On Violence* (New York: Harcourt, Brace, Jovanovich 1970), 37.

Sabotage

The rise of cyber attacks has made it easier to distinguish between violent and non-violent attacks. But sabotage, contrary to Stone's argument, does not rest on this distinction. Sabotage is the deliberate attempt to weaken or disable an economic or military system. The means used in sabotage may not always lead to physical destruction and overt violence. Sabotage may be designed to merely disable machines or production processes temporarily, and explicitly avoid damaging anything in a violent way. Again I gladly take Stone's advice and go beyond the Cold War. The question of sabotage and violence, even if only directed at machines, was controversial among syndicalists in the early twentieth century. Delaying production was one thing; destroying property was something else, something that could have dire consequences, legal as well as political ones. In America, political opponents had accused the radical syndicalists of relying on crude violence to achieve their goals. Some labour organizers considered it therefore necessary to distinguish between violence on the one hand and sabotage on the other. Arturo Giovannitti, a prominent Italian-American union leader and poet, argued for the latter in the foreword to the 1913 English translation of Émile Pouget's much-noted book *Sabotage*. Sabotage, Giovannitti wrote, was:

> Any skilful operation on the machinery of production intended not to destroy or render it defective, but only to disable it temporarily and to put it out of running condition in order to make impossible the work of scabs and thus to secure the complete and real stoppage of work during a strike.[5]

Sabotage is this and nothing but this, he added, using the language of political activism rather than the language of a scholarship, 'It has nothing to do with violence, neither to life nor to property.'[6]

Such subtle differences made sense in theory. In practice it was often difficult to distinguish between permanent destruction and temporary disablement – for several reasons, two of which will serve to highlight the novelties of sabotage by cyber attack. The first reason is the difference between hardware and software. If temporarily interrupting a process required damaging hardware, then the line between violence and sabotage became hard to draw. Cyber attacks, by contrast, restrain violence and make that line easier to draw: software attacks by default

[5]Émile Pouget, and Arturo M. Giovannitti, *Sabotage* (Chicago: C.H. Kerr & Co. 1913), 6.
[6]Ibid.

maliciously affect software and business processes by exploiting insecure systems, as Gary McGraw outlined – damaging hardware and mechanical industrial processes through software-attack, as Dale Peterson's response shows, is a highly specialized, bespoke, and more difficult undertaking.[7] Second, online attacks also made it easier, or possible in the first place, to isolate sabotage from volatile group dynamics. Remote cyber sabotage is highly unlikely to escalate into real bloodshed or street violence, as was not uncommon for the syndicalists – activist and perpetrators of code-borne sabotage, by contrast, may not even be physically present at the targeted site.

At closer examination the opposite of 'cyber war' is taking place: the rise of cyber attacks *reduces* the amount of violence and violent expertise embedded in sabotage, espionage, and even subversion – and, paradoxically, makes these activities more cost-efficient in the process.[8]

Note on Contributor

Thomas Rid is a Reader in War Studies at King's College London. A book based on the original article will be published in April 2013 under the same title.

Bibliography

Arendt, Hannah, *On Violence* (New York: Harcourt, Brace, Jovanovich 1970).

Hobbes, Thomas, *Leviathan* (London: Penguin 1996 [1651]).

McGraw, Gary, 'Cyber War is Inevitable (Unless We Build Security In),' *Journal of Strategic Studies* 36/1 (February 2013), <http://dx.doi.org/10.1080/01402390.2012.742013>.

Passerin d'Entrèves, Alessandro, *The Notion of the State* (Oxford: Oxford University Press 1967).

Peterson, Dale, 'Offensive Cyber Weapons: Construction, Development, and Employment,' *Journal of Strategic Studies* 36/1 (February 2013), <http://dx.doi.org/10.1080/01402390.2012.742014>.

Pouget, Émile and Arturo M. Giovannitti, *Sabotage* (Chicago: C.H. Kerr & Co. 1913).

Rid, Thomas, 'Cyber War Will Not Take Place,' *Journal of Strategic Studies* 35/1 (February 2012), 5–32.

Rid, Thomas, *Cyber War Will Not Take Place* (London: Hurst Publishers 2013).

Stone, John, 'Cyber War *Will* Take Place!,' *Journal of Strategic Studies* 36/1 (February 2013), <http://dx.doi.org/10.1080/01402390.2012.730485>.

[7]Gary McGraw, 'Cyber War is Inevitable (Unless We Build Security In),' *Journal of Strategic Studies* 36/1 (February 2013), <http://dx.doi.org/10.1080/01402390.2012.742013>; Dale Peterson, 'Offensive Cyber Weapons: Construction, Development, and Employment,' *Journal of Strategic Studies* 36/1 (February 2013), <http://dx.doi.org/10.1080/01402390.2012.742014>.

[8]For a more detailed outline of this argument, see Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst Publishers 2013).