Zbigniew Brzezinski

# THE CYBER AGE DEMANDS NEW RULES OF WAR

## A system to check covert violence is needed, writes Zbigniew Brzezinski

The two centuries since the Congress of Vienna have seen the gradual codification by the international community of the “rules of the game” for guiding interstate relations, even between unfriendly countries. Their basic premise has been the formula “don’t do to me what you don’t want me to do to you”. However, technological advances mean that today those rules are being dangerously undermined. The international system is at risk.

After the age of Metternich, Talleyrand and Castlereagh, elaborate understandings developed about the transition from formal peace to war. These involved carefully scripted exchanges of diplomats, rules about the treatment of prisoners of war and eventually even a shared definition of war crimes. Implicit in all this was the notion that while war and peace are fundamentally different conditions, both still need rules of conduct.

In more recent times, the use of nuclear weapons has made the distinction between the two more dramatic. The destructiveness of these weapons was without precedent but paradoxically that encouraged more cautious behaviour on the part of the states that possessed them. The existence of such weapons also created a new global hierarchy with a few nuclear states at the top and the rest below.

Today, the interstate rules of the game are degrading. Highly sophisticated capabilities for inflicting violence on remote targets, as well as cross-border, state-sponsored terrorism, are undermining the clear demarcation of what is permissible and what is not. Scientific advances have also increased the potential scope of acts whose perpetrators may not be easily identified and which may not be intercepted in a timely fashion.

Indeed, the world community is witnessing an increasing reliance by states on covert acts of violence without declarations of war. Leaders can now use long-distance air drones for lethal strikes across national borders against targeted individuals, occasionally killing civilians, too. The sophisticated dissemination of computer viruses can disrupt the military industrial assets of rivals. States can commission unacknowledged assassinations of foreign leaders and of scientists engaged in weapons development. They may back hacking of foreign institutions for intelligence purposes as well as of private business entities to gain commercial advantages.

Some states are also experimenting with more comprehensive cyber warfare designed to disrupt the operational infrastructure of targeted states, as in the case of the assault on Estonia and its banking

institutions in 2007. A rogue but technologically sophisticated state can now gain the capacity to launch a non-lethal but paralysing cyber attack on the socioeconomic system and the most important state institutions of a target country.

The dangers inherent in the degradation of the already vulnerable international system cannot be overstated. Social chaos, with paralysing fear magnified by uncertainty as to its origins, could spread. Making matters potentially even worse, such degradation is not the product of one or another particularly menacing state. Rather, it is the consequence of the rising vulnerability of the global system to cumulative pressures: technological innovation, massive and increasingly impatient populist upheavals and a shift in the distribution of geopolitical power.

In that volatile context, competing state tends to be subjective in judgments of their own conduct. There are lessons to be learnt from the onset of the nuclear weapons age. After the end of the second world war in 1945, the US wisely abstained from a pre-emptive attack that would have exploited its atomic monopoly but would probably have had monstrous consequences. But self-restraint ushered in a Soviet effort to gain first nuclear equality then superiority. America's admirably consistent determination to prevent the latter, as well as probably also the rise of a nuclear-armed but increasingly anti-Soviet China, compelled the Soviet Union to settle eventually for verifiable nuclear weapons parity.

An open discussion of today's novel risks to global stability might still help to avert unprecedented disasters. Responsible governments with a stake in global stability and technological capacity need to convene a process designed to set rules that inhibit the drift towards covert acts of aggression. As the world's foremost innovator, the US should take the lead.

But to make that process productive, the US itself – while resisting the temptation to do to others what America condemns others for doing – must make certain that its vulnerabilities are not easily exploited by adversaries that are difficult to identify. It is perplexing that the US, which apparently is able to use computers to inject undetectable viruses into sensitive foreign targets, seems so vulnerable and so uninformed regarding foreign hacking into its assets.

Calm and determined deterrence – including intensified efforts credibly to identify perpetrators as well as readiness in effect to retaliate in kind – must be the point of departure for new and genuinely reciprocal rules of the game. The need for such rules is becoming urgent.

*The writer was national security adviser to US president Jimmy Carter and is the author of 'Strategic Vision: America and the Crisis of Global Power'*