The Guardian

The age of cyberwar is here. We can't keep citizens out of the debate

David E Sanger

Unlike nuclear weapons, there is no clear protocol for when cyberwarfare should be used, or how to respond to an attack

Sat 28 Jul 2018 14.00 AEST

In almost every classified Pentagon scenario for how a future confrontation with Russia and China, even Iran and North Korea, might play out, the adversary's first strike against the United States would include a cyber barrage aimed at civilians. It would fry power grids, stop trains, silence cellphones and overwhelm the internet. In the worst-case scenarios, food and water would begin to run out; hospitals would turn people away. Separated from their electronics, and thus their connections, Americans would panic, or turn against one another.

The Pentagon is planning for this scenario because it knows many of its own war plans open with similarly paralyzing cyber-attacks against our adversaries, reflecting new strategies to try to win wars before a shot is fired. Glimpses of what this would look like have leaked out in recent years, partly thanks to Edward JSnowden, partly because a mysterious group called the Shadow Brokers – suspected of close links to Russian intelligence – obtained terabytes of data

containing many of the "tools" that the National Security Agency used to breach foreign computer networks. It didn't take long for some of those stolen cyberweapons to be shot back at America and its allies, in attacks whose bizarre-sounding names, like WannaCry, suddenly appeared in the headlines every week.

Yet the secrecy surrounding these programs obscures most public debate about the wisdom of using them, or the risks inherent in losing control of them. The government's silence about America's new arsenal, and its implications, poses a sharp contrast to the first decades of the nuclear era.

The horrific scenes of destruction at Hiroshima and Nagasaki not only seared the national psyche, but they made America's destructive capabilities - and soon Russia's and China's - obvious and undeniable. Yet even while the government kept the details classified - how to build atomic weapons, where they are stored, and who has the authority to order their launch - America engaged in a decades-long political debate about when to threaten to use the bomb and whether to ban it.

Those arguments ended up in a very different place from where they began: in the 1950s the United States talked casually about dropping atomic weapons to end the Korean war; by the 80s there was a national consensus that the US would reach for nuclear weapons only if our national survival was at stake.

So far, there has been no equivalent debate about using cyberweapons, even as their destructive power becomes more evident each year. The weapons remain invisible, the attacks deniable, the results uncertain. Naturally secretive, intelligence officials and their military counterparts refuse to discuss the scope of America's cyber capabilities for fear of diminishing whatever narrow advantage the country retains over its adversaries. The result is that the United States makes use of this incredibly powerful new weapon largely in secret, on a case-by-case basis, before we fully understand its consequences.

Acts that the United States calls "cyber network exploitations" when conducted by American forces are often called "cyber-attacks" when American citizens are the target. That word has come to encompass everything from disabling the grid, to manipulating an election, to worrying about that letter arriving in the mail warning that someone - maybe criminals, maybe the Chinese - just grabbed our credit cards, social security numbers and medical histories, for the second or third time.

During the cold war, national leaders understood that nuclear weapons had fundamentally changed the dynamics of national security, even if they disagreed on how to respond to the threat. Yet in the age of digital conflict, few have a handle on how this new revolution is reshaping global power.

During his raucous 2016 presidential campaign, Trump told me in an interview that America was "so obsolete in cyber", ignoring, if he was aware of it, that the United States and Israel had deployed the most sophisticated cyberweapon in history against Iran. More concerning was the fact that he showed little understanding of the dynamics of the grinding, daily cyber conflict now under way - the short-of-war attacks that have become the new normal. His refusal to acknowledge Russia's pernicious role in the 2016 election, for fear it would undercut his political legitimacy, only exacerbates the problem of formulating a national strategy.

But the problem goes far beyond the Trump White House. After a decade of hearings in Congress, there is still little agreement on whether and when cyberstrikes constitute an act of war, an act of terrorism, mere espionage or cyber-enabled vandalism.

Technological change wildly outpaces the ability of politicians - and the citizens who have become the collateral damage in the daily combat of cyberspace - to understand what was happening, much less to devise a national response. Making matters worse, when Russia used social media to increase America's polarization in the 2016 election, the animus between tech companies and the US government - ignited by Snowden's disclosures four years earlier - only deepened. Silicon Valley and Washington are now the equivalent of a divorced couple living on opposite coasts, exchanging snippy text messages.

Great powers and once-great powers, like China and Russia, are already thinking forward to a new era in which cyber is used to win conflicts before they appear to start. They look at quantum computers and see a technology that could break any form of encryption and perhaps get into the command-and-control systems of America's nuclear arsenal. They look at bots that could not only replicate real people on Twitter but paralyze early-warning satellites.

From the NSA headquarters at Fort Meade to the national laboratories that once created the atomic bomb, American scientists and engineers are struggling to maintain a lead. The challenge is to think about how to defend a civilian infrastructure that the United States government does not control, and private networks where companies and American citizens often don't want their government lurking - even for the purpose of defending them.

What's missing in these debates, at least so far, is any serious effort to design a geopolitical solution in addition to a technological one. In my national security reporting for the New York Times, I've often been struck by the absence of the kind of grand strategic debates surrounding cyber that dominated the first nuclear age. Partly that is because there are so many more players than there were during the cold war. Partly it is because the United States is so politically divided. Partly it is because cyberweapons were created by the US intelligence apparatus, instinctively secretive institutions that always err on the side of overclassification and often argue that public discussion of how we might want to use or control these weapons imperils their utility.

Some of that secrecy is understandable. Vulnerabilities in computers and networks - the kind that allowed the United States to slow Iran's nuclear progress, peer inside North Korea, and trace Russia's role in the 2016 election - are fleeting. But there is a price for secrecy, and the United States has begun to pay that price.

It is impossible to begin to negotiate norms of behavior in cyberspace until we too are willing to declare our capabilities and live within some limits. The United States, for example, would never support rules that banned cyber espionage.

But it has also resisted rules prohibiting the placement of "implants" in foreign computer networks, which we also use in case the United States needs a way to bring those networks down. Yet we are horrified when we find Russian or Chinese implants in our power grid or our cellphone systems.

"The key issue, in my opinion," says Jack Goldsmith, a Harvard law professor who served in George W Bush's justice department, "is the US government's failure to look in the mirror."

David E Sanger is the chief Washington correspondent for the New York Times. He is the author of The Perfect Weapon