THE WALL STREET JOURNAL.

https://www.wsj.com/articles/beijing-will-give-you-cold-war-nostalgia-11572909192

OPINION | GLOBAL VIEW

Beijing Will Give You Cold War Nostalgia

Nuclear deterrence was simple compared with the fluid nature of cyberwarfare.

By Walter Russell Mead

Nov. 4, 2019 6:13 pm ET

America's 21st-century competition with China is likely to be more dangerous and more complex than its old Cold War with the Soviet Union. This is partly because China's economic power makes it a much more formidable and resourceful opponent than the U.S.S.R., and partly because the technological environment has changed so dramatically in the past generation.

The development of nuclear weapons and intercontinental ballistic missiles shaped the Cold War. The resulting nuclear "balance of terror" kept the Cold War cold; neither power was willing to risk total annihilation. Arms-control talks became a centerpiece of superpower relations as both sides sought to stabilize the nuclear balance.

The information revolution has brought new dangers to the fore. Cyberweapons can devastate their targets, crashing power grids and transportation networks, paralyzing financial systems, and destroying the functionality of anything from hospitals to government offices. The development of these weapons is much harder to control and their use much more difficult to deter.

It isn't hard to know where a nuclear missile comes from. Cyberattacks are harder to trace and can easily be pinned on proxies. It is also harder to retaliate—one key to deterrence. U.S. companies and government agencies are daily subjected to cyberattacks from a variety of criminal groups and governments around the world. Should the U.S. launch retaliatory strikes against countries that commit cyberaggression against us? If so, what's the proper magnitude of response? If the

retaliation is too weak, it won't deter future attacks. If it is too strong, it may trigger an escalation that could be very hard to control. Deterrence is difficult to establish in the murky, ever-evolving cyberworld.

Arms control will also be much trickier in the brave new world of e-warfare. "Trust but verify," said Ronald Reagan, and that was possible though sometimes quite difficult in the Cold War. The sheer size of the industrial activities necessary to build up a nuclear force or a missile-delivery system made it possible for the U.S. and the Soviet Union to agree on verification measures. Cyberweapon programs are extremely difficult to detect, they bear fruit relatively quickly, and they are cheap compared with nuclear programs and even conventional arms. Negotiating verifiable cyber control treaties will be much harder than reaching Cold War-era nuclear arms-control agreements. Even if deals between superpowers can be reached, that won't stop the cyber arms race. Smaller countries, along with well-funded terror and even organized-crime groups, can develop significant cyber capabilities.

Rapid technological change makes a workable system of cyber arms control even more difficult to achieve. The sophisticated malware of 2012 is junk programming today, and changes in the way the internet works and how governments and companies use it come so quickly that nobody really knows what offensive and defensive capabilities will be needed in five or 10 years. Under these circumstances, neither governments nor companies can afford to limit their research-and-development programs.

Finally, the cyber arms race is directly linked to economic prosperity in a way that the Cold War arms race was not. During the Cold War, money spent on developing and deploying nuclear weapons and missile-delivery systems was seen, sometimes incorrectly, as a drag on the civilian economy. The desire to save money helped bring both sides to the arms-control bargaining table, and the burden of defense spending on the fragile Soviet economy helped persuade Mikhail Gorbachev that the Soviet Union needed to end the Cold War.

Cyber spending is different. Investments in research and development aimed at cyberwar bring direct and substantial benefits to civilian tech industries. The internet itself began as a Pentagon-funded project through the Defense Advanced Research Projects Agency's predecessor, and in the tech world the distinction between the race to achieve supremacy in militarily useful technology and in civilian technology has largely collapsed. As large and small powers across the world grasp the degree to which IT is the key to both national defense and national prosperity, defense-related cyber spending will grow.

The consequences will extend well beyond the defense industry. Investment in cutting-

edge IT capabilities, turbocharged by the link between those capabilities and national defense, will likely accelerate the cascading series of disruptions that the information revolution brings to the civilian economy. Automation, driverless cars and other potent innovations will come all the faster as government investment helps drive technological advances. Those disruptions in turn will fuel the social and political turmoil that threatens the stability of governments around the world.

After 9/11, American policy makers would sometimes speak nostalgically about the simpler problems of the Cold War. They'll come to miss those days all the more as the U.S.-China competition heats up. Dreadful as it felt to those who waged it, the Cold War took place in less dangerous times.