Cyber Warfare and Nuclear Weapons: Game-changing Consequences?

Sico van der Meer

In 2010, the U.S. Air Force lost computer communication with 50 Minuteman nuclear ballistic missiles for one hour, fortunately without any consequences.[1] In 2012, British researchers discovered that Chinese-manufactured computer chips used in military weapons systems, nuclear plants, etc., all over the world contain a secret "backdoor" that could facilitate disabling or reprogramming the chip remotely.[2] It is possible that such computer chips are also being used in nuclear weapons systems. These are only two examples of incidents of cyber threats regarding nuclear weapons that have become public, but probably more incidents in various nuclear weapon states remain unreported.

Most nuclear weapons systems were designed decades ago, when manipulations of computer networks, or cyber attacks, were an almost non-existent threat. Nowadays, cyber threats are everywhere, and one may expect that they have consequences for the stability of nuclear weapons systems as well. Considering the many unknowns of the still evolving issue of cyber threats, it is hard to measure how serious the risks are, but it cannot be excluded that, over the long term, they may have "game-changing" effects on the perceived value of nuclear weapons. This contribution briefly discusses two potential consequences of this phenomenon: cyber operations targeting nuclear weapons systems, and cyber operations replacing nuclear weapons. In conclusion, some potential policy options to deal with these consequences are presented.

Cyber Operations Targeting Nuclear Weapons

The most obvious cyber threat to nuclear stability is the risk of sabotage of nuclear weapons systems. One could think of cyber attackers feeding incorrect information into systems and – maybe far-fetched but not unthinkable – even taking control of the weapons. Various parts of nuclear weapons systems could be targeted, for example command and control systems, alert systems, launch systems, and target-positioning systems. Scenarios in which alert systems are hacked and show a massive nuclear attack by adversaries may lead to an accidental nuclear conflict, especially in states with automated warning systems attached to nuclear weapons on so-called hair-trigger alert. It is also conceivable that hackers are able to manipulate the coordinates of (pre-programmed) targets of nuclear missiles, or to spoof GPS-like systems that some missiles use to calculate their positions vis-à-vis their targets. Currently, there is no evidence that any state or non-state actor is able to successfully perform such manipulations, but considering the fast developments in the cyber arena, in the near future it might well be possible.

In the worst-thinkable scenarios, these possibilities may cause the inadvertent use of nuclear weapons, and/or use against unintended targets. In less dramatic scenarios, the perceived vulnerabilities of the nuclear weapons systems may affect nuclear stability. Especially the deterrent value of nuclear weapons may decrease, if potential adversaries think they have options to manipulate these weapons when being used, and/or when the possessor of the nuclear weapons suspects that adversaries can. It is hard to forecast the effects of such decreasing nuclear deterrence. On the one hand, it may encourage nuclear disarmament because the weapons are more or less perceived as being obsolete and/or dangerous; on the other hand, it may lower the threshold for using large numbers of nuclear weapons if this is perceived as strengthening the deterrent value to some extent.

Cyber Operations Replacing Nuclear Weapons

Another destabilizing effect of tools for digital manipulation, or cyber weapons, is their asymmetric nature. While currently only nine states (supposedly) possess nuclear weapons, cyber weapons can be obtained, developed, or used by any state or non-state actor; they are relatively cheap, risk-free, and easy to operate. This has two consequences.

First, cyber weapons may become a new kind of Weapon of Mass Destruction – or maybe it would be better to call them Mass Weapons of Destruction. It is to be expected that within a few years – thanks to the rapid, continuing digitalization of the world – cyber attackers could harm entire societies. Cyber weapons may not be able to cause the same level of deadly destruction as nuclear weapons, but they may be very powerful – think of serious, combined sabotage of energy and water supplies as well as communication,

transport, and payment systems, and so on. If this scenario were to become reality, it is conceivable that nuclear weapons would be regarded as outdated, expensive weapons that could be replaced by cheaper cyber weapons with more or less the same deterrent effect.

Second, nuclear weapons may not be able to deter cyber attacks.[3] Until today, convincing attribution of cyber attacks has been very problematic. This makes retaliation for cyber attacks hard as well; because of potential "false flag" operations (deliberately producing fake traces pointing to someone else), there is a serious risk of retaliating upon an innocent party. In case of large-scale cyber attacks that disrupt an entire society, retaliation with nuclear weapons may thus be even more problematic. Moreover, cyber weapons might well be used by non-state actors with no obvious territory to target, nor much to lose from any (nuclear) retaliation. From this perspective, nuclear weapons may lose part of their deterrent value.

Policy Options

To limit the potentially destabilizing effects of cyber threats on nuclear weapons, various policy options can be considered by the international community (especially the nuclear weapon states):

- Nuclear weapon missiles could be de-alerted and retargeted to hazard-free locations such as oceans to prevent inadvertent use because of cyber attacks. This will also increase the response time (especially in cases where there are automated alarm systems), enabling decision-makers to carefully check all circumstances before launching. To prevent manipulation via the cyber domain, human decision-makers must always be in the loop with regard to the possible use of nuclear weapons.
- Confidence-building measures (CBMs) among nuclear weapon states as well as toward non-nuclear weapon states could be developed to ensure that cyber attackers cannot cause incidents by manipulating nuclear weapons systems. These CBMs could deal with issues such as reliable emergency procedures to prevent inadvertent use after the control over any nuclear weapon is lost or manipulation is detected. Nuclear weapon states can no longer get away with statements such as "trust us, our nuclear weapons are safe"; they should offer at least some transparency concerning basic cyber security measures.
- Increased intelligence-sharing among nuclear weapon states regarding non-state actors trying to manipulate nuclear weapons systems via the cyber domain, cooperation in cyber forensics, and the sharing of best practices and lessons-learned regarding the cyber security of nuclear weapons systems.
- International standards could be developed on what minimum effects a cyber attack should have to qualify for military retaliation, including wording on if/when nuclear weapons could be used for that. An important issue in this regard is what evidence must be provided in order to engage in legitimate retaliation. In addition, one could think of establishing a neutral multilateral organization that inquires into and verifies the forensic evidence of large cyber attacks.

Theoretically, an international ban could be considered on embedding secret malicious codes or circuitry in products that could be activated any time (for example, in the event of war). Currently, this does not seem to be realistic though, because of serious problems with the verification and enforcement of such a ban.

1 Larry Shaughnessy and Chris Lawrence. "Air Force lost some communication with nuclear missiles." *CNN News*, 27 October 2010, accessed 8 September 2016. http://edition.cnn.com/2010/US/10/26/nukes.lost.communications/.
2 Sophie Curtis. "Cambridge researchers uncover backdoor in military chip." *Techworld*, 29 May 2012, accessed 8 September 2016. http://www.techworld.com/news/security/cambridge-researchers-uncover-backdoor-in-military-chip-3360617/.
3 Neil C. Rowe. "The attribution of cyber warfare." In *Cyber warfare. A multidisciplinary analysis*, ed. James E. Green (Oxford: Routledge, 2015), 61–72.