Why an escalating cyber-battle could risk nuclear war - Nuclear attacks could be part of our response in the future, but currently, the use of the weapons is highly unlikely by Alan Woodward - The Telegraph - March 19, 2021:
- https://www.telegraph.co.uk/technology/2021/03/19/escalating-cyber-war-could-risk-nuclear-war/

Carl Sagan perfectly encapsulated the **nuclear arms race** when he likened it to two sworn enemies standing waist deep in gasoline, one with three matches, the other with five.

In other words, nobody can be the first to use nuclear weapons as it would lead to mutually assured destruction (MAD). However, one could argue that the concept of MAD prevented World War III.

Several decades after the Cold War, we find ourselves with new **technologies** emerging at ever greater speeds.

We know that other countries seek to develop a range of technologies that, whilst not nuclear, could be used as weapons of mass destruction.

The current fleet of four Vanguard-Class nuclear-powered submarines are due to be replaced by a similar number of Dreadnought-Class boats in the 2030's CREDIT: PA Wire [see photo above]

A technological arms race

Our reliance on electronic devices makes us more vulnerable to attacks and makes it probable that technology may emerge that could send another country back to the Stone Age. People would die, property would be damaged and the impact could last for years.

As the first duty of a government is to protect the people it serves, how should a government prepare to defend against such an eventuality? Do you enter another arms race, matching each new form of weapon with your own?

In the cyber realm, the UK government has already signalled their intention to do precisely this in their **2016 Cyber Security Strategy**. It makes it clear that the UK would continue developing and deploying cyber capabilities against those who used similar technologies to do this country harm.

Advanced Persistent Threats | The world's most dangerous hackers

A government must strategise for such extreme situations and give itself the flexibility to respond with what it already possesses. Should such a potentially devastating technological threat emerge, the alternative is to accept that you could be held to ransom by whomever possesses it.

Previous generations of weapons of mass destruction, be they chemical, biological, radiological or nuclear, all had the potential to do the user harm as well as those against whom the weapons were used. Not so with cyber-attacks.

Nuclear response

However, cyber-attacks are not currently ‘cyberwar’. Recent rhetoric seeking to equate the two has led us to the situation where some have read the UK government's Integrated Review and inferred that a cyber-attack could be met with a nuclear response.

You can never say never, of course, but we are some considerable way off any cyberweapons being capable of wreaking the sort of destruction that would elicit a nuclear response from the UK.

The fact that such inferences are being drawn is a warning that all stakeholders need to be careful about the language they use around cyber-attacks. There is a world of difference between penetrating a system to conduct espionage and turning the national electronic infrastructure against the people who rely upon it.

At a glance | The Royal Navy’s submarine fleet

During the Cold War, another nuclear war doctrine was developed and continues to be used in war games today. It assumes that if conventional weapons are used in a dispute, nuclear weapons can be used in a limited response - a dangerous doctrine, as it required great restraint if it were not to escalate to all-out mutual destruction.

But it is an attempt to consider a proportionate or staged response, regardless of the type of weapon used to initiate the conflict. This type of thinking would be well-employed in a conflict sparked by cyber capabilities.

There is another factor to consider: attribution. There are relatively few members of the nuclear weapons club. Our monitoring systems know from whom and where such attacks come, if airborne; we also know who is capable of producing nuclear weapons. This is not the case with cyber-enabled attacks.

Hidden hackers

In the cyber realm, it can take considerable time to uncover who was truly behind an attack, not least because one bad actor can lay false flags suggesting a third party.

One can even imagine a scenario where a bad actor, knowing that two other adversaries will overreact, conducts an attack in which these adversaries will destroy each other without the original bad actor taking any blame or suffering any consequences.

In any future conflict where cyber-attacks play a pivotal role, governments will take their time to respond.

Deterrence will be multilayered and will be based upon proportionate response. However, deterrence is based upon the idea that if you launch an attack that devastates a country, you will suffer a similar fate.

At that point, how your opponent returns the devastation upon you is likely to be moot, but everyone knows all options would remain available in such situations.

Alan Woodward is a computer security expert and visiting professor at the University of Surrey. The University of Surrey received a £5m donation to its 5G Innovation Centre from Huawei in 2014.