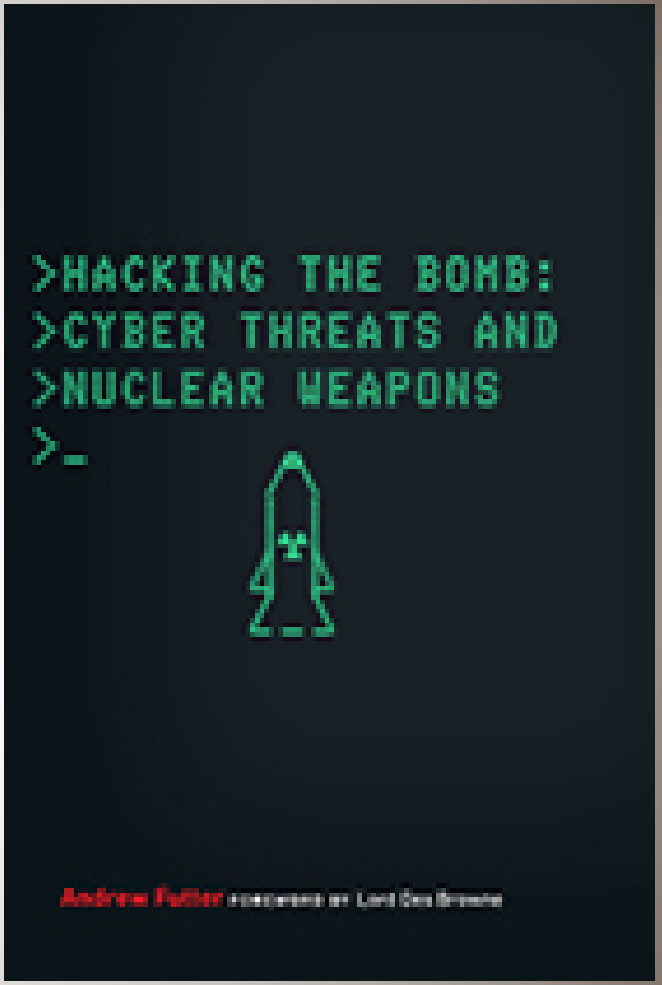
Hacking The Bomb

11 Things You Need To Know About Cyber Threats and Nuclear Weapons

Dr. Andrew Futter, ajf57@le.ac.uk

https://www2.le.ac.uk/departments/politics/people/afutter



UNIVERSITY OF LEICESTER

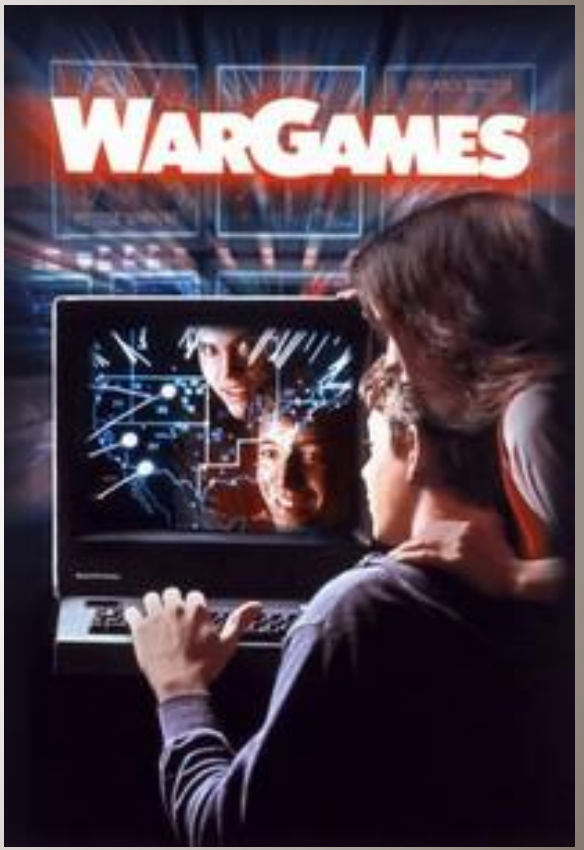
Introduction: The Cyber-Nuclear Nexus

Questions abound:

- Could hackers break into systems and cause a nuclear launch or prevent weapons being used?
- Could systems be spoofed electronically, and operators and decision makers tricked into making wrong and potentially fatal decisions?
- Could nuclear secrets be vulnerable to cyber-spies and would-be proliferators?

- And in what ways might they do this?
- What exactly does the threat look like, and what is vulnerable in what ways and to whom?
- How much of the hype should be believed?
- And what are the best ways to manage this challenge?

"Three decades after the sci-fi film was released, had the War Games scenario finally become reality?"



1. Cyber is Contested; This Causes Problems

There is no one accepted definition of “cyber”, and analysts and even states often talk past each other when using the term:

- For some, cyber is purely actions through the internet, for others it is bound up with information warfare, while it could refer to the current information age that we are living in.
- This makes understanding, let alone responding, to different threats very difficult.
- It is also often leads to hype and worst-case scenario thinking. Cyber 9-11 or cyber Pearl Harbour for example.

It is probably best to think of cyber as **comprising a set of tools or operations as well as a broader context**.

- The question then is not so much which cyber technologies can do what – although this is clearly important. But rather, how the changed context alters the way that we understand and interact with the world, and thus, how nuclear weapons are thought about and managed.

Because of this it often makes more sense in practice to work backwards from the phenomenon, threat or challenge being analysed and use that as a basis for cyber analysis.

- Above all, it is essential that there is clarity when the cyber moniker is used.
- There is even a case for getting rid of the term cyber all together…

“As far as the cyber, … we should be better than anybody else, and perhaps we're not.”

“The security aspect of cyber is very, very tough. And maybe it's hardly do-able. But I will say, we are not doing the job we should be doing, but that's true throughout our whole governmental society. We have so many things that we have to do better, Lester and certainly cyber is one of them.”

Donald Trump, 2016

2. Cyber and Nuclear are Different

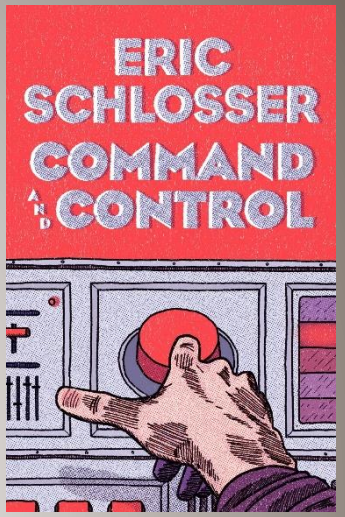
It is common to compare cyber and nuclear and seek to draw lessons from our nuclear past to inform our cyber future. But while many of the questions may be the same, the answers are likely to be very different. The often-used analogy is therefore flawed:

1. The major difference is the extent of the damage that either can cause; so far no one has died as a direct result of cyber attacks
2. Targets are likely to be different; with a few exceptions, sophisticated cyber-attacks will have to be specialised and rely on prior knowledge of the target.
3. There is no established tradition of cyber non-use, or a likely way in which the verification of previous arms control treaties could be replicated. There is no analogy of MAD in cyberspace either.
4. Part of the reason for this is the importance of transparency; nuclear strategy is based on an adversary being able to see what you have deployed and where; cyber strategy relies on keeping capabilities secret – as soon as they are revealed they lose deterrent value.
5. The vast majority of cyber operations fall well below what we might consider as military or warfare, and it is often more useful to view cyber as a context rather than as a weapon or tool.

"The tendency to view the two as equivalent leads to dangerous and erroneous comparisons and recommendations."

Weapons of Mass *Disruption*	**Weapons of Mass *Destruction***
Temporary: Stuxnet	Huge casualties: Hiroshima & Nagasaki
Specialized	Indiscriminate
Ongoing	Nuclear taboo/ non-use
Secret	Transparent
Crime & Nuisance	Warfare & Strategic

3. Some Cyber Challenges are Inherent



Although we tend to associate cyber threats with hacking and weapons, a major component of the challenge is inherent and won't involve attackers

- There are two reasons for this;
  - The delicate balance of nuclear systems between always being ready to be used but never by accident or without authorisation means they will never be as secure as they might be, and;
  - The more complex these systems become, the more likely they are to go wrong – this can be thought of as ***"normal nuclear accidents".***

The challenges of the digital age are exacerbating rather than fundamentally transforming issues of nuclear security and strategy.

- A good example of what might go wrong is the problems experienced at NORAD in the 1980s where faulty computer chips and the accidental loading of a training tape caused serious false alarms.

Keeping nuclear systems tightly coupled with warning sensors and ready to fire at short notice is clearly a big risk in the cyber age.

- This is complicated by the fact that many of today's nuclear systems are far more complex and difficult to understand than those of the past.

Nuclear modernisation is a double-edged sword and should not be pursued automatically or viewed apriori as a good thing.

"Unfortunately, most warning systems do not warn us that they can no longer warn us."

Charles Perrow

4. Cyber Threats Are Diverse

Rather than a single cyber threat, we are better thinking of a threat spectrum: ranging from nuisance and hacking, through crime, espionage, DDoS, up to physical attacks, seeking damage or destruction, and maybe even warfare.

- Often these are lumped together, creating strawman arguments and a lack of understanding. It also complicates the response to these challenges.
- The majority of activities in cyberspace occur at the lower end of this spectrum. Only a handful of cyber operations could be thought of as strategic and causing damage. There has been no cyber warfare.

We can also think of attackers in the nuclear realm as seeking either to *enable* something – for example, either directly or indirectly cause a nuclear launch; or seeking to disable systems (i.e. stop them from working through sabotage or by denying key information).

- In most situations, states are likely to try to carry out disabling attacks, while non-state actors are likely to seek to carry out enabling actions. These build on and take advantage of measures for positive and negative nuclear control noted earlier.
- Both could also pursue cyber-nuclear espionage for different purposes – possibly proliferation.

States are likely to be more capable of attacking systems directly, and of taking the time to develop specific malware, implant it and keep it concealed, while non-state actors would probably seek to attacks systems indirectly – such as by meddling in the information space - this is because there are often far easier and cheaper methods for terrorist to achieve their aims.

5. Air Gapping is Not a Panacea

There is a common belief that by air gapping systems they will be safe against cyber attackers. While air gapping certainly makes things harder, these systems are still vulnerable.

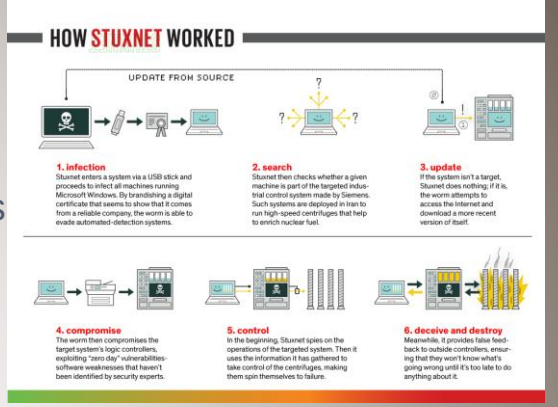
- Stuxnet entered an air-gapped system at Natanz. It is likely that a contractor was duped into transferring infected files and therefore jumping the air gap.

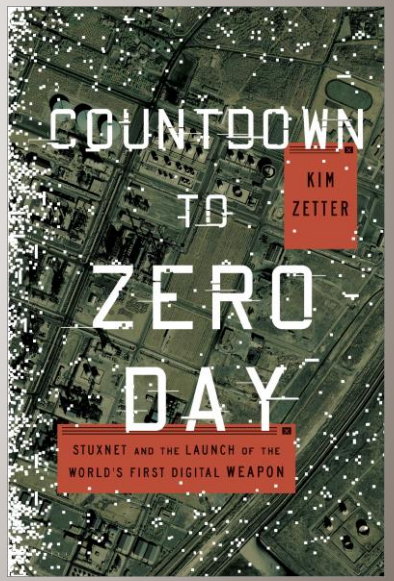
Another example is the UK Trident submarines - officials have told me that they can't be hacked because once on patrol they are somewhere under the sea disconnected from computer networks.

- But this overlooks the fact that these submarines have to be designed, built, and rely on numerous different types of computer systems for which software and coding has to be written. Logic bombs, hardware Trojans, or other malware could potentially be placed and lay dormant until required. It would be very hard to ever find this.
- These subs also regularly come into port for upgrades and maintenance, which offers another opportunity for attackers. While in port, I understand that they are occasionally connected to networks at the base.
- Cyber-attacks need not cause the sub to launch a missile or for it for explode, but might instead target the reactor, navigation systems, or other computers essential for its normal functioning.

The increasing dependency on CoTs and software not built in house presents a risk across the nuclear weapons infrastructure.

- My research suggests that some countries rely on software and hardware built abroad in their most sensitive systems, including for nuclear weapons.





UNIVERSITY OF LEICESTER

6. Espionage and IP theft is the biggest risk

Espionage is by far the biggest cyber threat

- Although the challenge of protecting *operational* and *design* secrets is not new
- A diversification of methods (Internet but also USB drives etc…)
- "Hoovering" and new economies of scale

Challenge is for both hacking and information and systems security more generally

- Again air gapping does not equal protection
  - The human/ insider threat also remains key

"Cyber-nuclear espionage" began in the 1980s

- "The Cuckoo's Egg (1986)
- "Kindred Spirit/ Wen Ho Lee" –W88 (1998)
- Has expanded exponentially since

The implications are however mixed…

Steal Sensitive Information	Defend Against/ Combat Systems	Aid Proliferation	Precursor to Cyber Sabotage
Cuckoo's Egg (1986)	*Dutch hackers (1990-1)*		*Syrian nuclear programme (2007)*
BARC hack (1998)	*Kindred Spirit (1995-8)*		*Olympic Games, Flame & Duqu (2000s)*
Moonlight Maze (1999)			
Titan Rain (2005)			
Buckshot Yankee (2008)			
Zeus Trojan (2011)			
Iran hacks IAEA (2011)			
Anonymous hacks IAEA (2012)			
Shady RAT (2011)			
Zeus Trojan (2011)			
Attacks on US defense contractors/ nuclear labs (2000s-)			
Attacks on US/ Israeli BMD systems (2010s-)			

7. Deterrence Can Play a Role, But…

The majority of cyber threats are best dealt with through cyber hygiene and good practice, defence and security, and where necessary law enforcement.

However, it is possible that some cyber operations cross the line and might be considered as acts of war or as military operations. In these cases, deterrence by punishment could have a role to play.

- The thing to remember with cyber deterrence is that it applies only in certain circumstances; also, it is not simply an either-or but rather something that is graduated.

Attribution is often held as the major reason why deterrence can't work in cyberspace, but attribution is not zero-sum, and depends on a number of different variables, chief among them time and forensic capacity.

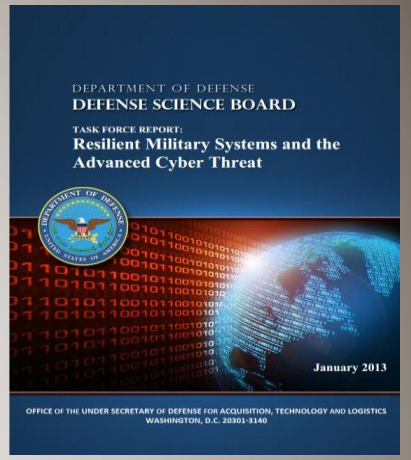
Where deterrence can become complicated is when considering a proportional response:

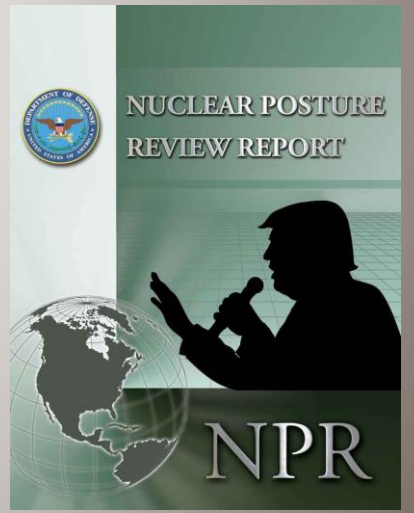
- For example, it might be very difficult to respond "in kind" to a cyber-attack, and more likely a state would simply respond with the most appropriate tools at its disposal.
- This then leads to questions of cross domain deterrence.

Thus, while the idea of threatening nuclear retaliation to a cyber-attack may seem overblown, as a response to an existential attack or an attack that involves cyber – it is not impossible.

- US, Russian, Chinese and UK deterrence policy all remain underpinned by nuclear weapons. None have specifically ruled it using nuclear to respond to cyber.

Deterrence by Punishment + Deterrence by Denial





UNIVERSITY OF LEICESTER

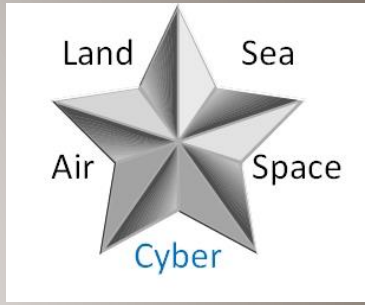
8. Viewing Cyber as “Separate” is Unhelpful

We are also unlikely to ever see a pure “cyber war” and we shouldn’t be tempted to view strategic cyber threats in isolation or as a separate “domain” of military operations.

- While cyber capabilities may be used on their own for low-level operations; testing defences, espionage, nuisance etc.; at the military or strategic level, cyber-attacks will almost certainly be used in conjunction with other forms of military force, to augment them, to “prepare the battlefield”, and as a force multiplier.
  - This means that we must assume cyber operations will play a part in all future conflict and crises, but alongside other forces.

At the strategic level, we should think of cyber as a component of a new suite of ***advanced non-nuclear weaponry*** – all of which have been facilitated by the latest information revolution.

- These systems include ballistic missile defences, various precision strike weapons, new undersea and space weapons, AI, and more exotic future capabilities.
- Taken together these advanced non-nuclear forces are creating considerable pressures for nuclear relations and global nuclear order.



“We are unlikely to ever see a pure cyberwar where geek fights geek on an electronic battlefield.”

James Lewis

UNIVERSITY OF LEICESTER

9. Cyber Threats are Most Dangerous in a Crisis

Most cyber operations, and even those conducted against nuclear systems, are likely to be manageable or at least less risky in periods of calm; but will be exacerbated considerably during a crisis, especially a nuclear one.

1. State actors would likely seek to disable an opponent's key systems before military operations – this might involve actions to "prepare the battlefield"
   - This will create uncertainty and possibly pressures for pre-emptive attacks, and potentially fears of "use it or lose it".
   - During conflict, states might also inadvertently attack dual use systems, or cyber operations might be misinterpreted or spill over

2. Terrorists, other non-state actors or third parties, might seek to interfere in various ways; spoofing systems; conducting false flag attacks, flooding the battlefield with misinformation etc., intending to cause a crisis to escalate.

3. The reliance of modern states and their militaries on computerised communications systems will make signalling and controlling operations much more difficult on a cyber-battlefield.
   - This is likely to create further problems for crisis management and possible unintended escalation.

This suggests that what we think we know about nuclear crisis management needs to be reassessed in light of this new context.

10. Humans Are a Key Part of the Challenge

Irrespective of the hi-tech nature of the challenges posed by cyber and the way that the threats are often conceptualised, humans are an are absolutely fundamental part of the puzzle.

- Humans design and build computer systems, write coding and create software, enter data, operate these machines, and make decisions based on the information that they provide.
- Humans also unknowingly give away personal information, click on infected emails, download malware, insert infected drives into systems and are therefore a key way of "bridging the air gap".
- Above all, humans are clearly an obvious, and often the easiest target for would-be attackers. Much easier than seeking to bypass firewalls, develop and exploit zero-day exploits, or utilise other exotic ways of jumping the air gap.
- This might either be wittingly in the role of an insider threat or mole or unwittingly, such as it likely to have been the case with Stuxnet.
- This might involve some sort of cyber social engineering too.

"Ultimately, computers don't think – at least not yet – they do what they are programmed to do."

UNIVERSITY OF LEICESTER

11. An Emerging Norm of "Hacking the Bomb"?

In the past few years there is has been an increasing recognition that cyber operations might be used in the strategic and nuclear sphere.

- The discovery of the Stuxnet attack on the Iranian nuclear centrifuges at Natanz in 2010 is clearly the best example of this, but it is also likely only to be the tip of the iceberg, and probably only part of a broader cyber and electronic campaign targeting the Iranian nuclear programme.
- It also seems very likely the similar operations have and are being conducting against North Korea.
  - Last year, suspicions arose that US-led cyber-attacks might be responsible for a succession of failed North Korean missile launches.

This is part of a plan for US "full spectrum missile defence" where "left of centre" cyber capabilities will augment traditional kinetic plans for interception, and at the same time, another component of the US global strike programme

- The US is ahead at the moment, but it is far from clear that it will remain so in the longer term, and it is hard to see other leading cyber competitors, including those potentially hostile to the US and UK won't follow suit.

These actions risk setting a dangerous precedent and creating a far more unstable global nuclear environment.

- We could be moving towards an era of mutually unassured destruction or (MUD)…

"…[global strike] is probably [the ability to be] any place on the face of the earth in an hour" while the "high end is any place on the face of the earth in about 300 mili-seconds – that's cyber."

US Gen. James Cartwright

Conclusion and Recommendations

The response to the cyber challenge in the nuclear realm is necessarily multifaceted:

1. There needs to be some sort of agreement on terms and the nature of the threat and perhaps an accepted glossary.
2. A considerable amount of the challenge might be ameliorated through better cyber hygiene and good practice – this might even be shared between actors. This also involves recognising the central role played by humans.
3. The need for cyber and nuclear (and other defence) communities to speak with each other, possibly across borders.
4. Train and deploy specialists at nuclear facilities, and conduct regular outside red teaming.
5. Establish a cyber global early warning centre to share data, intelligence and good practice
6. Consider the development of certain norms and moratoria – for example, an agreement not to attack nuclear C2 with cyber – that benefit everyone.
7. Cyber and other emerging technologies with strategic potential should be included in arms control discussions and taken account of in international agreements. That said the arms control frameworks of the past may not be the most suitable for today.

In the emerging cyber-nuclear nexus, it makes sense to keep nuclear facilities simple, separate and secure, and not follow the allure of technological determinism.

"It is suicidal to create a society dependent on science and technology in which hardly anybody knows anything about the science and technology."

Carl Sagan

UNIVERSITY OF LEICESTER

My New Book: Hacking the Bomb

"If you are bothered by the fact that our top security officials cannot determine with high confidence whether computer malware or other hacking could cause Russian, Chinese, or U.S. nuclear missiles to be illicitly fired, you should read this book. If you are bothered by the fact that cyber operations could confuse leaders into launching nuclear missiles during a crisis, you should read this book. If you are not bothered because you are not aware of such dangers, you should read this book. Professor Futter asks all the right questions about the myriad dangers that information warfare poses to the command and control of nuclear forces, and illuminates the answers to the extent that current knowledge allows. His important and provocative book also connects the cyber issues to the major risks of nuclear instability and accidents, providing rich context for his analysis. A cross between historical investigation, policy analysis, and theory, this is a must-read volume for anyone who cares about this perilous new threat to mankind."—***Bruce G. Blair***

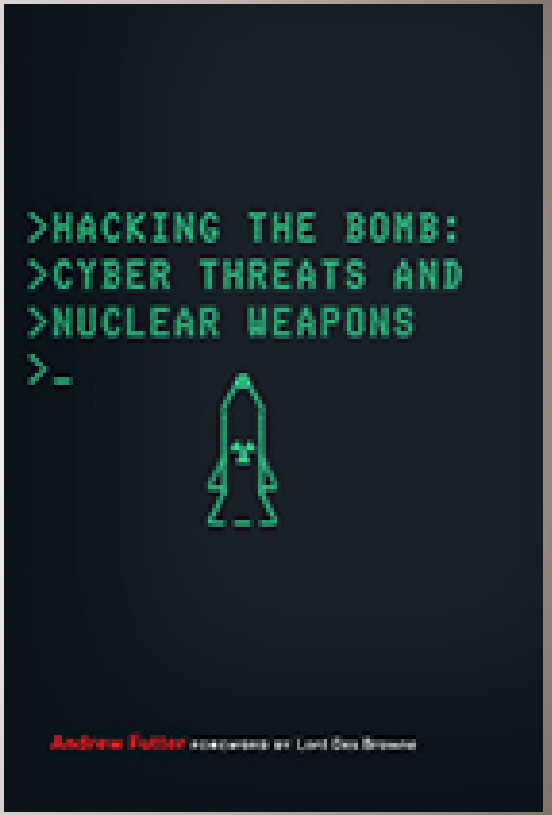
"Nuclear strategy is hard - but cyber operations makes it harder. In this thorough and insightful work, Andrew Futter skillfully weaves the many threads binding cyberspace and the nuclear establishment to urge caution for those who would ignore or promote cyberwar on nuclear capabilities. Strategists of all flavors, take note."—***Martin Libicki,***

"Will resonate well with those interested in nuclear weapons and cyber threats alike. For all others, the content serves as a well-researched point of reference for the intersection of these two ever-present topics in the modern security landscape."—***Proceedings***

"Futter's valuable book surveys the new dangers and also considers how states might deter cyberattacks on critical infrastructure. He stresses the importance of securing sensitive nuclear information and of keeping control systems as simple as possible and separating them from other networks."—***Sir Lawrence Freedman, Foreign Affairs***

Available from: http://press.georgetown.edu/book/georgetown/hacking-bomb.

30% Discount Code: TGU



UNIVERSITY OF LEICESTER