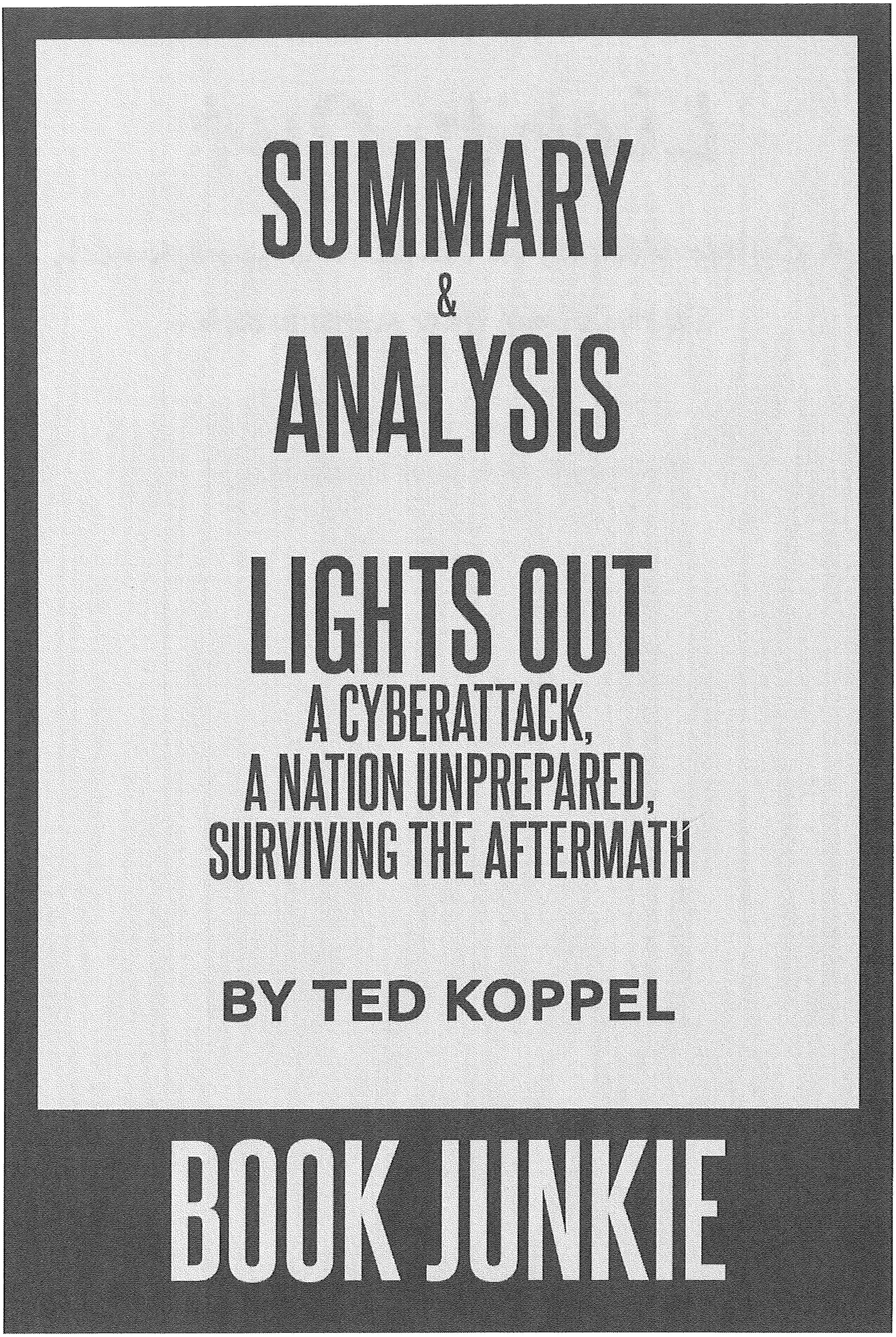
SUMMARY
&
ANALYSIS

LIGHTS OUT
A CYBERATTACK, A NATION UNPREPARED, SURVIVING THE AFTERMATH

BY TED KOPPEL

BOOK JUNKIE

R. MOREL
8.4.16



SUMMARY & ANALYSIS

LIGHTS OUT

A CYBERATTACK, A NATION UNPREPARED, SURVIVING THE AFTERMATH

BY TED KOPPEL

BOOK JUNKIE

Lights Out

A Cyberattack, A Nation Unprepared, Surviving the Aftermath

By Ted Koppel

Summary & Analysis by Book Junkie

Contents

Authorial Background

Ted Koppel, full name Edward James Koppel, was born February 8, 1940 in England to German Jewish parents. He came to the United States in 1953, his parents being refugees of World War II. Koppel is a reporter, television journalist and author, and was the anchor for *Nightline* from 1980 until 2005. He graduated from Syracuse University with a Bachelor of Science degree and from Stanford University with a Master of Arts degree in mass communications research and political science ("Ted Koppel Biography"). Koppel has won 37 Emmy Awards, six George PeaBody Awards, 10 du-Pont Columbia Awards, nine Overseas Press Club Awards, two George Polk Awards, and two Sigma Delta Chi Awards in broadcast journalism ("Ted Koppel"). Before *Lights Out*, Koppel wrote *Nightline: History in the Making of Television* in 1996, exploring the creation of the show Nightline. In 2001, he published his memoir *Off Camera: Private Thoughts Made Public.* Koppel is married to Grace Anne and has four children.

Cultural Context

In 2016 United States, post-9/11 paranoia has mostly passed and citizens' biggest political fear (besides Donald Trump) is now rooted in government overstep, specifically regarding privacy. By contrast, we put more private information about ourselves out into cyberspace than ever before – address, phone numbers, credit cards, and even social security numbers. Millennials, the most technologically savvy generation, are more at risk of cyber theft than any other generation. More importantly, the entire infrastructure of the United States depends on the functioning of the cyber web. Although a few outlier countries are still reported to be building up their nuclear capabilities, most nations have moved on, accepting the threat of retaliation and complete destruction. The new and developing method of attack is now cyberterrorism, and several countries are becoming very skilled. Ironically, the United States themselves paved the way for this method of terrorism when they conducted a cyberattack with Israel on Iran's nuclear program, the first ever major cyberattack.

Plot Summary

Part 1: A Cyberattack

Koppel begins by introducing a scene where a cyberattack has been waged on the electric grid of the United States. There's mass chaos, no information available, and no end in sight. Our dependence on the electric grid for our power, water, and health infrastructure puts us in an incredibly vulnerable position, especially since other nations and individuals have the ability to wage a cyberattack against the electric grid. Unfortunately, the public does not have this threat on their radar, and convincing the public of this danger is nearly impossible with mainstream biased media. You can find an expert to prove your opinion no matter what it is. Legislation regarding this kind of cyberattack has made it past the house, but has become stuck in the senate.

As an example of real life power grid attacks, Koppel offers Pacific Gas and Electric Company (PG&E), whose Metcalf Transmission Substation had their cables cut and their transformers knocked out by AK-47 assault rifles. This substation powers the entire Silicon Valley. Fortunately, power was rerouted so the grid was fine, but the damage could have been far worse. Some contend that this proves the power grid is more resilient than others think, but the president of the FERC (Federal Energy Regulatory Commission) believes that this may have been a rehearsal attack, since the actions taken show that the attackers were well trained. Alarmingly, in 2004, Russian military personnel warned the EMP commission that North Korea had recruited Russian scientists to develop its nuclear and EMP attack capabilities. These threats have not been taken seriously, nor have suggestions by the EMP Commission to prepare for these dangers been taken seriously.

Current regulations regarding cybersecurity are minimal and don't cost much to the company if violated. The FERC also has limited jurisdiction, as the companies that distribute power directly to the local population are not subject to federal regulations. Koppel explains that the main vulnerability of SCADA (Supervisory Control and Data Acquisition) systems used for our power grid are "attack surfaces". He does so by comparing malware and viruses to an actual virus, Ebola. When an American man was infected, his two nurses wore two layers of protective gear and were entirely covered, but there was a space on their neck where the fabrics met. Both nurses contracted the virus, because their protective gear had an "attack surface", a point of vulnerability. Similarly, SCADA systems have attack surfaces that exist both through the interconnectedness of SCADA systems and in human error, such as an employee who uses an unsecure thumb drive or phone to bring information from home to work for upload.

There is widespread disagreement among industry professionals on the nature of the threat of cyberattacks on the power grid. There are some defenses that are coordinated between the private and the public sector, including CRISP (Cybersecurity Risk Information Sharing Program), but this system is quite small and includes only a very small percentage of companies. It will take years before everyone is involved. Some believe that the threat is overstated by the security industry, but those in security say they are only called in for help once security has already been breached. These professionals aren't conjuring ideas of easy cyberattacks, they are responding to actual incidents. The threat is real. However, there continues to be dispute among officials in the industry. Perfectly protecting the power grid is not cost efficient and ignores privacy concerns, so companies are very hesitant in moving forward.

Certain unintended consequences extend far into the cyber age, and can be compared to the unintended consequences of the invention of the car. There are unnecessary deaths every single year, but as a society we accept this threat and minimize it as much as possible for the sake of the convenience found in cars. The internet has had similar consequences. In the wrong hands, millions of people have been hacked for private information and/or for monetary gain. Since no one agrees on the risk of cyberattack, Koppel decided to discuss the issue with an insurance specialist, a person in the business of objective risk assessment. Jain contended that although the risk is there, the risk is also too new and too large for insurance companies to stick more than just a toe in the water.

Cyberattacks come down to opportunity, capability, and motive. Opportunity meaning a vulnerability in the system, which Koppel demonstrates there are plenty of. Capability is demonstrated by the development of the means for cyberwarfare in multiple nations. And motive comes from several areas, namely the United States' involvement in the entire international community. As far as our defense is concerned, we have a great issue preparing for battle because we often put profit and privacy before security, and we operate under the constrictions of a democracy.

Unlike the understood threat of mutual destruction that comes with nuclear warfare, no similar understanding exists yet in regards to cyber warfare. We don't fully understand all it involves, and it's not just a few blocs of countries with cyber capabilities like there is with nuclear capabilities. It's everyone. With nation-states, there's the threat of retaliation and damaged relationships, but with independent actors or terrorist-oriented nation-states, actors can hide from retaliation behind anonymity thanks to the nature of cyber warfare, and there's no vested interest in maintaining certain aspects of a relationship with the United States. All these factors make cyber warfare wildly unpredictable and threatening, but defense teams are more concerned with current issues, not potential ones, and it's understandable why.

Part 2: A Nation Unprepared

The weakest links in our power grid are large power transformers (LPT), which cost millions of dollars, are usually 30-40 years old, are typically made overseas, and are thus nearly impossible to transport. Plans if these LPTs fail are minimal and experimental at best. There really is no set protocol if a widespread cyberattack on the power grid were to take place. Different administrations disagree on how to handle the situation or if it really even is a threat. Some believe people would be easily transported to safe areas, while others believe that the transition would not be so smooth and that lives definitely would be lost. There's not much individuals can do because of how interconnected our systems make us.

In a state of emergency, we are not prepared for more than a few days. For example, we only have a certain number of ready-to-eat meals, and we can't stockpile more because they have an expiration date of five years. Most of our money is spent on post-emergency efforts, rather than emergency prevention. Rural America is generally more self-reliant, so Koppel thought maybe they would be better prepared. Not so much. Even in this area Koppel experienced several unsuccessful calls and attempts to get information from the Red Cross, FEMA, and the Department of Homeland Security about emergency preparedness for individuals. Citizens are encouraged to have plans for two to three days' worth of disaster, but no more than that.

Part 3: Surviving the Aftermath

Like the Biblical story of Noah's Ark, people are often skeptical of oncoming but unproven disaster, and so preparedness then becomes an individual responsibility. However, a movement of doomsday preppers have risen, all preparing for different types of disasters. It's a complicated balance, because people need to worry about themselves at a certain point, but it also takes a community of different skill sets to be fully prepared. Prepping is clearly a rich man's game at the moment, with multi-million dollar projects to improve family sustainability and provide security. While this doesn't help poor and urban families, it does show what kind of projects can be done for a more sustainable future.

In smaller, western areas, self-reliance is the norm. Individuals and families have their own systems, but also are willing to help neighbors in need. These better prepared areas could be useful in a time of cyberattack, but the issue comes with integration. These smaller, western towns are usually fairly homogenous in terms of race and socioeconomic status, so a sudden influx of "outsiders" may not go over smoothly.

The Mormon Church has a long history of persecution that drives them to prepare for the unexpected. The mantra of the Mormon Church is preparedness. If you're prepared, then you have nothing to fear. Everyone in the community works together to prepare their families as well as the community for any time of need. The Mormon Church across the United States and Canada is entirely self-sufficient, with expansive storehouses of home grown food, and even their own factories for production. Several of their operations contain the name "Deseret" in the title, which is from the Book of Mormon and means "honeybee". "Just like the honeybee, Mormons work and live within a self-sufficient, collaborative, and highly productive community" (196). Having such large storehouses, the next question for the Mormon Church is what they would do if people tried to steal their supplies in the case of a disaster. Because of their history of being both victim and perpetrator, the Church will not consider having an armed defense for their storehouses. They do not want to bring more controversy to the church. However, their instructions for their members are purposefully ambiguous. Members are permitted and sometimes encouraged to have a gun, but no policy or guidebook says what they should have the gun for, leaving the suggestion open to hunting purposes or even defense. Church leaders urge that the matter is between each individual and his heavenly Father, rather than a strict church doctrine regarding defense.

Until the general public and leadership are aware of the real threat of a cyberattack, no moves will be made. There are a couple ideas for preventive measures, but they would still take years to begin. One man wants to create the equivalent of a home security system for small to medium sized power companies. However, this would require information sharing between the government and the industry, which may not be legal. The other idea is to go back to having military bases produce their own power. With the right equipment, they could produce in excess and then supply that excess to government and emergency response agencies in the wake of disaster. Koppel argues that we should move decision-making and implementation power in this arena from the Department of Homeland Security to the far more competent NSA. However, this would further trigger privacy concerns given the public view of the NSA.

Much of the issue comes down to public outrage. Since no cyberattack of scale has occurred, citizens are far more concerned about privacy than security. In order for government to be responsive and take action, the pendulum of public outrage must swing towards security.

Epilogue: The Virtue of a Plan

Koppel grew up during the Second World War in England, so he was quite familiar with the civilian defense plans practiced on a community and nation-wide level. Although they were useless generally against attacks, they added to an important perception of preparedness meant to calm citizens and to send a message to the enemy that they would stay and fight.

He ends the book with this: "Acknowledging ignorance is often the first step toward finding a solution. The next step entails identifying the problem. Here it is: for the first time in the history of warfare, governments need to worry about force projection by individual laptops. Those charged with restoring the nation after such an attack will have to come to terms with the notion that the Internet, among its many, many virtues, is also a weapon of mass destruction."

Title Significance

The title *Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath* begins by painting an image of the effect of a cyberattack on the nation's power grid: darkness. The remainder of the title reflects the organizational break down of the book.

Themes and Focus Points

The threat of a cyberattack on the power grid and its treatment comes with several points of conflict:

Privacy v. Security

Government and industry professionals must work together and share information in order to adequately protect against a large-scale cyberattack. However, firms are hesitant to share information due to privacy concerns for the firm and for their clients.

Security v. Profit

Being prepared is expensive. For example, large power transformers cost millions of dollars and are thus not easy to keep as backups. It doesn't help their bottom line for firms to take on huge security projects.

Long Term v. Short Term

Along the same lines as the last conflict, it's much easier for firms and government agencies to focus on and prepare for the known short term rather than the unknown long term. It's hard to justify spending millions of dollars on a potential threat we don't even fully understand.

Offense v. Defense

Do we wait out the threat until we are actually attacked and then retaliate? Or do we take the time and resources to defend against an attack beforehand?

Individuals and Families v. Communities

In the event of some form of large scale disaster, do we focus only on protecting ourselves and our families, or do we lend a hand to help those around us? In order to truly be effective in disaster preparation, it takes a large group of individuals with different skills and resources working together. However, it's easy to go into protection mode and worry only about your family.

In addition to these conflicts, there are certain issues pertaining to the threat of cyberattack that are uniquely different from other forms of attack and terrorism.

Vulnerable Points

Our cyber system includes several vulnerable points, called "attack surfaces". The main attack surfaces arise when secure information is transferred through home devices rather than work devices. Unlike other methods of attack, these spaces vulnerable attack are largely due to human error.

Deniability

Cyberterrorism allows for anonymity. Hackers can make an attack from China look like it originated in Russia, which makes retaliation nearly impossible. This frees countries or groups who would otherwise fear retaliation or would fear losing certain aspects of their relationship with the United States to now be able to attack freely.

Interconnectedness

Unlike a bomb or a missile on an area of land, the interconnectedness of the cyber web allows for cyberterrorists to cause much more damage to a wider area than ever before.

Writing Style and Structure

Lights Out is divided into three sections. The first part, *A Cyberattack*, explains the nation's vulnerability to cyberattack as well as the history that paved the way for this vulnerability. Part two, *A Nation Unprepared*, investigates several government and industry organizations to find the lack of planning and preparation done for the instance of a large-scale cyberattack. Finally, *Surviving the Aftermath* explores communities of individuals who have taken to their own preparation plans, with a special focus on the Mormon church, in order to survive the aftermath of a cyberattack, or any disaster for that matter. Each chapter begins with a significant or piercing quote from the text, highlighting important points. Due to Koppel's professional background, the majority of the book consists of information obtained from interviews with government and industry leaders, as well as everyday civilians. The three-part structure of the book lends itself to easily provided context, and the interviews provide much credibility to Koppel's contentions about cyberwarfare.

My Thoughts on Lights Out

Lights Out provides an interesting insight to a threat I had never before considered. Koppel does a great job providing a historical and political context to the issue of cyberwarfare and the power grid, and does so in a way for the professional and the layman alike to understand. However, I was left unsatisfied with Koppel's third part to the book, *Surviving the Aftermath*. The preppers interviewed were incredibly wealthy, and the Mormon Church is a huge organizational structure with a long history of disaster preparation. Koppel offers no insight for urban city dwellers without these kinds of resources or connections. His only advice is to go to the mid-west, while conceding that we all couldn't possibly be accommodated. Some large-scale industry preparedness projects are explored, but none have begun the implementation stage and will take years to be effective. I would have liked to see more practical advice for the average American citizen.

Questions for Discussion

1. Do you think the threat Koppel depicts is a real threat or simply fearmongering?
2. Why do you think legislation regarding the security of the power grid have failed to pass?
3. What can be done to bridge the gap in perceptions on the actual threat of a cyberattack on the power grid?
4. How can the conflict between security and privacy be reasonably mitigated?
5. Brainstorm! Besides relocating, what can individuals in densely populated areas without enormous wealth do to prepare for a cyberattack on the power grid?

Significant Quotes

Part 1: A Cyberattack

Chapter 1: Warfare 2.0

"The assumption that the city, the state, or even the federal government has the plans and the wherewithal to handle this particular crisis is being replaced by the terrible sense that people are increasingly on their own. When that awareness takes hold it leads to a contagion of panic and chaos" (5).

"There are emergency preparedness plans in place for earthquakes and hurricanes, heat waves and ice storms. There are plans for power outages of a few days, affecting as many as several million people. But if a highly populated area was without electricity for a period of months or even weeks, there is no master plan for the civilian population" (5).

"To be dependent is to be vulnerable" (6).

"If, however, an adversary of this country has as its goal inflicting maximum damage and pain on the largest number of Americans, there may not be a more productive target than one of our electric power grids" (7).

"History often provides a lens through which irony comes into focus. The United States, for example, was the first and only nation to have used an atomic weapon, and it has spent the intervening decades trying to limit nuclear proliferation. And the United States, in collaboration with Israel, mounted a hugely successful cyberattack on Iran's nuclear program in 2008 and now finds itself dealing with the consequences of having been the first to use a digital weapon as an instrument of policy" (9).

"Prudence suggests that we at least consider the possibility of a cyberattack against the grid, the consequences of which would be so devastating that no administration could consider it anything less than an act of war" (10).

"It's [media bias] divisive and damaging to the healthy functioning of our political system, but it's also indisputably inexpensive and, therefore, good business" (13).

"It has never been more difficult to convince the American public of anything that it is not already inclined to believe" (14).

"Ours has become a largely reactive culture" (14).

Chapter 2: AK-47s and EMPs

"...if nine of the country's most critical substations were knocked out at the same time, it could cause a blackout encompassing most of the United States" (19).

"...the commission report estimating that only one in ten of us would survive a year into a nationwide blackout, the rest perishing from starvation, disease, or societal breakdown" (22)

"James Woolsey argued that protection of the national electric grid against an EMP attack is possible, that it is not prohibitively expensive, and that necessary congressional action is long overdue. In its 2008 report the EMP commission recommended that measures taken by the Defense Department to protect crucial military installations, including the installation of surge arrestors and Faraday cages, could usefully be applied to civilian infrastructure also. The commission estimated that protecting the national electric grid against an EMP attack would cost about $2 billion…no action was taken…" (23).

"In the endless competition for federal funding, Washington has grown inured to the chorus of lobbyists crying wolf on behalf of one cause or another" (23).

Chapter 3: Regulation Gridlock

"The federal agencies best equipped to monitor infrastructure for signs of cyberattack are precluded from doing so by laws that were designed to preserve privacy. When there are breaches of infrastructure security, corporations are protected by law against any mandate to share that information with competitors or the federal government" (27).

"This tension has resulted, in the electric power industry, in a high-stakes duel between corporations and government regulators, the consequences of which are cybersecurity regulations so patchwork and inadequate as to be one of the chief sources of the grid's vulnerability" (27).

"Because the system's maintenance and protection reside in so many different hands, though, and because its complexity has made each player more dependent on computerized control systems, the grid is also more vulnerable than it used to be…Leaders in the industry will argue that they have invested enormous resources in protecting their infrastructure, and they have. But smaller companies with lean profit margins are simply not inclined to spend a great deal on cybersecurity. The weakest links in this system tend to be the smaller companies with the poorest security and maintenance practices" (28).

"Cascading outages could compromise the systems of larger companies, quickly threatening the entire network" (29).

"American democracy rests on a foundation of competing tensions among local, state, and federal laws, and laws governing the electric power industry reflect those tensions" (30).

Chapter 4: Attack Surfaces

"…different companies are responsible for different phases of the process. The company that distributes electricity in one community, for example, can buy power from a number of companies generating electricity in other parts of the country. Breaking up the industry into a marketplace of interconnected parts introduced competition, which lowered prices. It also increased the system's vulnerability to cyber intrusion" (35).

"If you could hack into that computerized system and throw supply and demand out of balance, it could have devastating consequences" (36).

"To coordinate this, the industry has set up regional authorities, the regional transmission organizations and independent system operators, which monitor 'traffic' to ensure that no transmission lines in their area become overburdened. This monitoring process, while routine, also creates a dangerous point of vulnerability. If someone was able to hack into an RTO or ISO and deliberately overload the lines, the impact would be swift and physical" (37).

"The genius of the U.S.-Israeli attack lay in its ability to conceal the sabotage...The SCADA system controlling those nuclear centrifuges in Iran was manufactured by Siemens, as is much of the SCADA software used by the electric power industry in the United States" (40).

"A Verizon/Secret Service study concluded that two-thirds of companies across a spectrum of industries didn't realize they had been breached until someone outside the company informed them. Another study, conducted by the cybersecurity firm FireEye, found that it took on average 279 days before companies that had been breached came to realize it or were told by someone else" (42).

Chapter 5: Guardians of the Grid

"Certainly no one has a greater interest in protecting the security of the electric power industry than the industry itself – if only cost were not a factor and profit were not an essential ingredient of staying in business. It is not altogether reassuring, then, to consider that the only institution with real power to decide how the power industry is protected is the power industry...In evaluating industry regulations in 2012, the nonpartisan Congressional Research Service questioned the entire arrangement, calling it 'unusual' and observing that it 'may potentially be a conflict of interest' for an industry to legislate its own standards" (45).

"For any sort of cyber defense system to efficiently protect the electric power industry, information sharing has to be a two-way street. Corporations will have to get over their privacy and liability concerns and give government agencies the security data those agencies say they need in order to be effective. The military and intelligence agencies, in turn, need to make information relating to cyber threats available in real time, setting aside worries about jeopardizing sources and methods" (47).

"It is difficult to focus the attention of the power industry executives on speculative threats when there are so many existing problems to deal with" (49).

"Fama acknowledged that the distribution end has become more vulnerable as the entire system – from generating to distributing electricity – is increasingly digitized, but he argued that it was an unlikely target for a massive attack" (51).

"That, I pointed out, is just what the Iranian nuclear technicians believed as they watched television monitors showing normal operations, while in reality thousands of their centrifuges were spinning out of control. Air-gapping works unless and until an employee infects the system by bringing in a personal device – a thumb drive, say – from the outside" (53).

"...there is anything but unanimity within the industry on the issue of risk assessment" (56).

Chapter 6: What Are the Odds?

"There is now ample evidence that the law of unintended consequences applied as remorselessly in the realm of cyberspace as it does anywhere else" (57).

"'People always say we can add it on later. [But] you can't add security to something that wasn't designed to be secure'" (59).

"'You remember your kids in the backseat yelling so you and your wife couldn't talk? That's a distributed denial-if-service attack. That can be done with them not knowing much about your facility, only throwing packets of data at you. Overloading the system so you can't conduct business. If you're a stockbroker or a company that makes its living on the network, that's a huge problem" (61).

"'But from the insurance industry's perspective, the amount of exposure that we are willing to take on is nowhere close to the exposure that would come from these very extreme events.' With so much still unknown about the risks involved, his company may soon offer insurance against cyberattacks, but it will likely demand such a high premium that there will be few buyers" (66).

Chapter 7: Preparing the Battlefield

"Any successful attack combines three features: opportunity, capability, and motive" (69).

"In trying to find the proper balance between security and profit, many industries still incline toward a shortsighted emphasis on profit" (70).

"Civil libertarians, worried about real and potential violations of privacy, are often insufficiently focused on an even greater need to address external threats to liberty" (70).

"Like the *Time's* source, George Cotter believes that the rash of cyberattacks on U.S. banks during the summer and fall of 2014 does, in fact, constitute a warning from the Kremlin, related to events in Ukraine – a demonstration to Washington of what might follow if economic sanctions escalated" (73).

"A U.S. security firm, Crowdstrike, spent much of 2014 tracking a group of Iranian hackers. They found that the hackers had the potential capability not only to spy on but also to critically damage sensitive networks in the United States, Canada, Israel, India, Qatar, Kuwait, Mexico, Pakistan, Saudi Arabia, Turkey, the United Arab Emirates, Germany, France, England, China, and South Korea" (75).

"Among the key points in the report was that hundreds of thousands of domains registered to Iranian citizens or companies are hosted by companies in the United States, Canada, and Europe and are then used to conduct cyberattacks on America and its allies" (75).

"Arguably, though, none has ever been equipped with a weapons system as versatile, as potentially destructive, and as easy to deploy as the Internet" (78).

"There is similar agreement that the nation's cyber defense capabilities are more modest. It's a function, many believe, of operating within the constraints of a democracy" (78).

Chapter 8: Independent Actors

"As one moves down the capability scale of potential actors, though, a disturbing phenomenon becomes apparent. Iran, for example, presents somewhat less of a threat than China or Russia in terms of its capability but has far fewer overlapping interests with the United States. North Korea is yet several notches below Iran on the capability scale but has almost no interlocking interests with the United States and therefore even few restraints. In some ways most worrisome of all is the realm of individual hackers, whether independent or at least not visibly associated with a national government" (80).

"What distinguishes the terrorist organizations from the nation-states can be summarized in two words: *goals* and *consequences*" (81).

"It is precisely among young, educated radicals, warns Austin, that a new generation of cyber warriors will be recruited" (82).

"As damaging as the cyberattack on Sony may have been, it never constituted an obvious threat to national security. If, however, a skilled team of hackers can disrupt a large corporation in the entertainment field, what's to prevent them from launching equally devastating attacks on American infrastructure?" (84).

"What is most dangerous about Pyongyang and its mercurial leadership is not only its unpredictability but also its degree of immunity to cyberattack. North Korea has so much less to lose in a high-stakes cyber war than the cyber-dependent United States; it is neither easy nor particularly effective to isolate a hermit kingdom" (85).

"How ironic that the first acknowledged military use of cyber warfare is ostensibly to prevent the spread of nuclear weapons. A new age of mass destruction will begin in an effort to close a chapter from the first age of mass destruction" (88).

"Whatever limited reassurance we have that nuclear weapons remain under rational control does not apply to the use of cyber weapons" (89).

Part 2: A Nation Unprepared

Chapter 9: Step Up, Step Down

"The nature of the electric industry is such that is combines modern technology with antiquated equipment. Some of that equipment is so large, so expensive, and so difficult to replace that it constitutes an entire category of vulnerability. If there is one piece of hardware that deserves to be singled out as critical to the nationwide transmission of electricity, it is the large power transformer" (93).

"The industry has competitive, security, and antitrust justifications for its reluctance to share data; that reluctance, however, extends to sharing with the appropriate federal agencies" (94).

"Conservatively, there are thousands of aging transformers, most custom-built, unable to be ordered from a catalogue or mass-produced, each costing somewhere in the neighborhood of $3 million to $10 million. Add to this that there are only a handful of plants in the United States capable of building an LPT – as of this writing, ten such facilities. The vast majority of large power transformers are built overseas, and more than 75 percent of those purchased by the U.S. energy sector must be procured overseas. The estimated lead time, the time from production through shipping to delivery, is commonly between one and two years, and never less than six months…All of this combined to present a critical liability for the resilience of the United States power grid" (95).

"In the current climate of greater competition, and with management under pressure to return as much profit as possible to shareholders, the bottom line has taken priority over resiliency, especially among smaller and midsized companies" (97).

Chapter 10: Extra Batteries

"There have been, as of this writing, only four secretaries of homeland security. Each of them has conceded the likelihood of a catastrophic cyberattack affecting the power grid; none has developed a plan designed to deal with the aftermath" (104).

"We're so interconnected…it's not just me anymore: it's me and my neighbors and where I get my electricity from. There's nothing I can do that can protect me if the rest of the system falters" (105).

"This approach falters, however, when relevant federal agencies fail to provide for (or in some cases even contemplate) the difference in magnitude between the effects on the grid of any recorded natural disaster and the potential effects of a massive cyberattack" (113).

"The aftermath of a massive earthquake, though, bears very few similarities to the loss of a power grid to cyberattack. Where FEMA's presumed 9.0 earthquake would leave a city in rubble, with thousands of dead and injured, even the most massive cyberattack would inflict very little immediate physical damage…even buildings that appeared undamaged and infrastructure that had not been destroyed could be severely compromised" (114).

"We're not a country that can go without power for a long period of time without loss of life. Our systems, from water treatment to hospitals to traffic control to all these things that we expect every day, our ability to operate without electricity is minimal" (117).

Chapter 11: State of Emergency

"...bureaucrats are left with what he called the basic tools of government, 'which are extortion and bribes. Either I give you grant dollars to get you to do something you would not otherwise do, or I tax you to change behavior for what you will not otherwise do'" (121).

"The security implications [of getting first responders to work] are huge. You know, they're concerned about their families, they're concerned about their well-being. So over time when you talk about protecting the points of distribution, that all implies that government workers are showing up and do their jobs, and you can't guarantee that over a sustained period of time" (126).

"We tend to come up with funding after disaster strikes" (127).

Chapter 12: Press Six If You've Been Affect by a Disaster

"Among the findings [about Red Cross]: emergency vehicles taken away from relief work and staged as backdrops for press conferences; inadequate food, blankets, and batteries in locations where these were desperately needed; tens of thousands of meals thrown out because no one knew where to find the people who needed them" (132).

"If not the Red Cross, FEMA, or the Department of Homeland Security, where should the interested citizen turn?" (135).

Part 3: Surviving the Aftermath

Chapter 13: The Ark Builders

"For the most part, public reaction to the possibility of a massive cyberattack has not even risen to the level of apathy. Apathy suggests the awareness of a problem and the decision not to worry about it. We're not there yet" (139).

"There is, in any event, a growing movement around the country based on the assumption that neither government agencies nor private relief organizations can be relied upon in the event of any major disaster" (139).

"But preppers of every era have been outnumbered by the skeptics who tend to view their activities with a combination of fascination and amusement" (141).

"Certain conventions remain nonnegotiable: there must be a months' worth, if not years' worth, of potable water and nonperishable food, or, alternatively, the capacity to grow and hunt food" (144).

"The fact remains, however, that absent any guidance from Congress or the executive branch of government, beyond broad recommendations for weathering the first seventy-two hours or so, individual Americans have been left to select their own approaches to the prospect of a lengthy, widespread loss of electric power" (144).

"The idea of a prepper's movement is something of an oxymoron. For the most part, these are people who put a great deal of stock in individual responsibility. They anticipate government failure and are innately suspicious of large organizations. At the same time, in some quarters there is the recognition that long-term survival in the face of a widespread catastrophe requires a variety of skills – the establishment of what would amount to emergency communities" (150).

Chapter 14: Some Men Are an Island

"Craig Kephart is applying what he has – money, determination, and a great deal of time and effort – to sustain him and his family in the aftermath of disaster, in whatever form it comes. It would not be fair to suggest that these are the mindless expenditures of a wealthy dilettante. But what Craig has constructed and assembled in rural Missouri is clearly an enterprise beyond the means of most Americans" (161).

"The concept, called 'distributed generation,' is not unique to Andrew Rose. It envisions downsizing the current system of large-scale power plants to clusters of smaller generators spread across a broader area...None of this is going to be of any immediate value to a family in Chicago wondering how they will survive the loss of a power grid, but it provides a glimpse into a more sustainable future" (163).

Chapter 15: Where the Buffalo Roamed

"The point of visiting Wyoming was precisely that it is not New York or Los Angeles. It is not only a different environment, it is a different culture. Disaster preparedness is a matter of upbringing and common prudence. The skills that empower self-sufficiency are ingrained from childhood" (166).

"However romanticized this vision might have been, the fact is that Wyoming does have an unusually strong culture of both self-reliance and civic cooperation" (170).

"Neighborliness is more than a slogan here; it is, as it has always has been, an essential element of self-preservation in a challenging environment" (171).

"Underlying all expectations of survivability in a major city like New York is the assumption that underpopulated places such as West Virginia or Wyoming could, in extreme circumstances, absorb a couple of hundred thousand urban refugees" (177).

"To just assume, however, that the underpopulated rural regions of the United States are inclined or even able to absorb tens or hundreds of thousands of urban refugees - white, black, brown, many of them poor - is to place too much reliance on the notion of neighborliness" (178).

Chapter 16: The Mormons

"...it didn't go much beyond the notion that Mormon families were encouraged to keep a three-month supply of food and water on hand. There were also faintly ominous suggestions that the Church of Jesus Christ of Latter-day Saints had gigantic, strategically located storehouses filled with supplies" (179).

"The church is a highly disciplined, hierarchical organization" (180).

"They are encouraged to prepare for the days of tribulation as a matter of religious doctrine, but also as a direct consequence of historical experience" (181).

"When, during many of the religion's early years, that hostility manifested itself in the form of physical violence against church members, preparing for disaster became an essential element of survival; this ultimately matured into a matter of doctrine itself" (181).

"If you are without bread, how much wisdom can you boast, and of what real utility are your talents, if you cannot procure for yourselves and save against a day of scarcity those substances designed to sustain your natural lives?" (184).

"No group of comparable size comes close to matching the scale and organizational discipline of the Mormons' efforts to prepare for whatever catastrophe may come" (184).

Chapter 17: State of Deseret

"For the Mormons, this means starting with families, who are encouraged to prepare, over time, for unspecified emergencies. They are urged to gradually set aside enough food, water, clothing, and money to sustain themselves for three to twelve months" (187).
"What distinguishes the Mormons is their extraordinary focus on the integration of self-sufficiency and charity. That carefully layered structure is what gives the LDS church its impact and efficiency" (189).

"...if you are prepared you shall not fear. This is at the center of our religion, this scripture, to be prepared" (191).

"It would be the first of several instances in which I witnessed a determination not to consider or treat any member of the community as anything other than productive" (192).

"The church is independent of any outside supplier. What it donates, what it sells, and what it puts into storage all come from within a single ecosystem" (195).

"...Deseret. It's a term used in the Book of Mormon, meaning 'honeybee,' and it has symbolic resonance within the church. Honeybees, too, work and live within a self-sufficient, collaborative, and highly productive community" (196).

Chapter 18: Constructive Ambiguity

"We rely on who we rely on every day in a scenario [of violence] like that. I think we have to rely on the reaction of those who have the responsibility to police citizens, and that doesn't fall under us as a church. We've never built a preparation model that would talk about arming ourselves, or arming members of the church to defend..." (200).

"This is an organization that, in almost every other respect, stresses its self-sufficiency, its independence, its reluctance to depend on government assistance. The issue of self-defense, though, is toxic" (201).

"We're relying on all government agencies, really, to help protect our members of the church" (202).

"...each individual member rely on their relationship with their Father in heaven and know exactly what best to do" (204).

Chapter 19: Solutions

"The greater the level of self-sufficiency and the large the number of social networks able to function independently for at least a week or two, the more successful government relief efforts will ultimately be" (208).

"To establish a foundation with long-lasting, nourishing foods that have sustained needy families for generations – rice, wheat berries (and the grinder to make flour), beans – and large containers of water seems ridiculous in times of plenty, but it can become the difference between survival and starvation during an extended crisis...Eventually the supplies become part of a natural pattern – rotation of the older food into a pattern of daily consumption, always to be replaced with fresh supplies" (208).

"locate and establish the needs of the most vulnerable, determine the skills and assets of those willing to share either or both" (209).

"Law enforcement, fire departments, and teams of emergency medical workers are the ideal agencies to draw communities together in disaster preparedness" (209).

"In Keith Alexander's ideal world, his company would be running a cyber equivalent to the home security control center, monitoring the overlapping power company networks" (214).

"The operative question is whether Alexander's company could then legally pass that information on to the government or another power company, which would be equivalent to ADT calling the police or alerting a neighbor" (215).

"Unless there's a true crisis, we're going to move slow" (215).

"Since these modular reactors on military bases could produce more energy than they need, cooperative agreements could be worked out with local communities, providing emergency power to hospitals, police departments, and other first responders in the event that the grid goes down" (217).

"Anticipating and tracking external cyber threats to U.S. infrastructure should be, by virtue of capability if nothing else, the responsibility of the NSA" (220).

"We need to adapt to the realization that an as-yet-undetermined point a cyberattack on one of the nation's three electric power grids amounts to an attack on the United States" (221).

Chapter 20: Summing Up

"We are at one of those evolutionary stages in history that tracks the end of an era…for the first time in the history of warfare, small groups, even individuals, can undermine the critical infrastructure of a state" (223).

"The inability to quickly discover the identity of an aggressor undermines the threat of retaliation" (225).

"The leaders of democracies have always argued that they are operating at a disadvantage in their dealings with totalitarian governments. The Russians don't need to worry about infringing on the privacy concerns of their citizens or their critical industries" (229).

"What's at issue is whether we are prepared to surrender some of our privacy to our own intelligence agencies in order to protect against even greater intrusions from a growing array of external enemies. Until the general public is made to understand the scope of the actual threat, the natural inclination will be to preserve what we know and value, against what we still suspect may never happen" (230).

Epilogue: The Virtue of a Plan

"What mattered at the time was not so much the likelihood of actual survival as the perception of a ready-for-anything level of preparedness."

"Our points of vulnerable access are greater than in all of previous human history, yet we have barely begun to focus on the actual danger that cyber warfare presents to our national infrastructure."

Bibliography

Biography.com Editors. "Ted Koppel Biography." *Bio.com*. A&E Networks Television, n.d. Web. 23 Jan. 2016. <http://www.biography.com/people/ted-koppel-9368366#synopsis>.

"Ted Koppel." *ABC News*. ABC News Network, n.d. Web. 23 Jan. 2016. <http://abcnews.go.com/Nightline/News/story?id=128629>.

You Need To Read This Book because this will help you dive deeper into the world of Ted Koppel.

Emmy and Peabody Award Winner Ted Koppel offers an investigative insight into the threat of a cyberattack on the United States' power grid. Lights Out provides input from national and industry experts, as well as local community members as to our awareness of and preparedness for a uniquely unpredictable form of attack in the Internet age.

This summary serves as an accompaniment to Lights Out and offers insights to help you enjoy and understand this book.

Inside, you'll find helpful information on:
The Author's Background
Cultural Context
Plot Summary
Title Significance
Themes and Focus Points
Writing Style and Structure
Questions for Discussion
Significant Quotes

Disclaimer: This book serves as an accompaniment to the bestseller Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath by Ted Koppel. It is meant to broaden the reader's understanding of the book and to offer some insights which can easily be overlooked. You should order a copy of the actual book before reading this.

ISBN 9781520833118
90000
9 781520 833118