



Infrastructure Protection in the Ancient World

*What the Romans can tell us about their aqueducts,
What we may apply to our modern infrastructures*

By Michael J. Assante

Infrastructure Protection in the Ancient World

What the Romans can tell us about their Aqueducts –
What we may apply to our modern infrastructures

By Michael J. Assante

About the Author

Michael Assante is a sitting member of the Commission on Cyber Security for the 44th Presidency. As an Infrastructure protection strategist and adviser at the Idaho National Lab to the Department of Homeland Security, Department of Energy and Department of Defense, Mike researches and writes on issues related to homeland security and critical infrastructure protection. He is a former U.S. Naval Intelligence Officer and has also served as a Vice President and Chief Security Officer of a large U.S. electric utility.

Abstract

This paper provides lessons learned from ancient Roman attempts to protect the aqueduct, which was considered one of their most critical infrastructures. It also offers an analogy to modern day efforts in securing our own critical infrastructures, particularly the Nation's electric power grid.

Introduction

Contemporary societies owe much to the Romans. In fact, the western world has openly credited ancient Rome for our knowledge and application of the modern calendar, government, and public administration. We have also benefited from their engineering achievements like the arch¹, the invention of cement, and the road system that linked Europe.

As a security professional working with the government and assisting industry in understanding and developing strategies to protect critical infrastructures, I began speculating whether there might be other lessons we could learn from our early Roman predecessors relative to infrastructure protection. I became encouraged in my research since this ancient culture was the first to develop and administer public works and infrastructures that later became critical to the growth, stability and prosperity of the Roman Empire. These achievements obliged me to more closely investigate this historical period in search of modern day parallels.

There are three prominent Roman infrastructures that

have been recognized by historians, archeologists, and the common man; the road system, agriculture and food stores, and the most beautiful, yet practical Aqueducts². Given their import, could there be any poignant lessons that modern culture could take away from the story of ancient Rome and her infrastructures?

This article presents some of the lessons from ancient Rome and her aqueducts. Although not an historian, I will begin by exploring the role and importance of the aqueduct and how the Romans had regarded this infrastructure. Next I will review some of the major factors surrounding security of the aqueducts, and finally, discuss how the aqueducts went from being able to withstand threats to ultimately being rendered inoperable by them. This article is not historical in nature, nor is it meant to replicate the works of scholars. Instead, I have applied the work of historians and archeologists to derive sensible lessons in the context of modern day critical infrastructure protection. Also, this article is not a commentary on existing industry and government efforts to address security risks faced by our nation's infrastructures. It merely provides a different perspective from which to consider this important national issue.

Comparisons of ancient Rome and modern American systems are everywhere. But, are there enough relevant similarities and differences that we can study in hope of identifying issues and developing a better understanding of what might be at risk? Can we learn anything more from these ancient examples? Let's begin to explore and answer these questions.

Ancient Roman Aqueducts

Several of ancient Rome's most notable traits and accomplishments will factor into our study. Acknowledged for its science and engineering achievements, ancient Rome's rule by law and the unparalleled security it enjoyed for over 500 years is unprecedented. It should be no surprise that the still visible and impressive structures of the ancient water system stand as a testament to Roman engineering. What might be considered surprising is the fact that

¹ See glossary for definition.

² See glossary for definition and description.

some of these ancient structures are still in use today in various capacities.³

The Aqueducts were critical to ancient Roman civilization and its evolution from a regional power into a vast empire with transcontinental reach and influence. Rome's largest cities required the aqueducts to grow and sustain larger populations. While the early city of Rome had access to water from the Tiber River and wells for storage, this water supply was susceptible to pollution and eventually became insufficient to meet the demands as Rome became a geographically and culturally diverse trading center and attracted larger populations. The first Roman aqueduct was conceived to bring fresh water down from the hills surrounding Rome and is believed to have been constructed around the year 313 B.C.⁴ This construction coincided with the completion of the first major road, known as the Via Appia. There would eventually be a total of eleven aqueducts built to service the city of Rome over the course of ancient history from the republic through the empire. These eleven structures were able to service the entire city and enabled the population to grow to well over a million inhabitants. Aqueducts would also be constructed to develop and support other suitable population centers through out Roman territories.

Academic experts have concluded that Rome could not have built cities as large as it did without the aqueducts and that without them, some of their cities would not have existed at all.⁵ The Romans explicitly understood the critical importance of the aqueducts, and in the first century, a public administrator named Sextus Julius Frontinus was appointed to oversee their management and care. Frontinus wrote, "with such an array of indispensable structures carrying so many waters compare, if you will, the idle pyramids or the useless, though famous, works of the Greeks." Frontinus had much to be proud of as it has been estimated that during the height of production and distribution, the water system delivered an astounding tens of millions of gallons of water every day.² It is vital to note that the Romans understood the importance of the aqueducts that served them. Frontinus characterized them as

"indispensable," much like we have defined certain critical infrastructures in the United States today.

The aqueducts were critical to Roman society because of the essential service they provided and because they could not be easily replaced. It is believed that a long aqueduct like the Eifel (supplying what is present day Cologne) at over 320,000 Roman feet long (approximately 60 miles) took 2,500 workers over 16 months to complete.⁶ As a society ruled by law, Rome's recognition of the importance and vital nature of the aqueduct is best understood from the inscription found in Lyons, France, which reads "By command of Emperor Trajanus Hadrianus Augustus, no one is permitted to plough, sow, or plant within the space determined for protection of the aqueduct." It is significant to note that Rome chose to develop precise legal protections to safeguard this critical infrastructure. To provide an idea of how ubiquitous and significant these components of critical infrastructure were, it is said that at Rome's peak, nearly 200 cities within the empire received portions of their water supply by aqueducts, far surpassing the capability of any civilization before or after for nearly another 2 millennia.³

For a more probing review of Rome's efforts to protect its critical infrastructure, let's ponder an important question: Did the Romans proactively address and provide for infrastructure security when building the aqueduct? The answer is a resounding "Yes". In fact, how they afforded security for the infrastructure along with what changed and why is an important lesson for us to consider. It isn't inconsequential that the first aqueduct was built entirely underground (see Figure 1). The reason



Figure 1. Roman aqueduct built underground as a security measure.

³ United Nations of Roma Victrix, "Aqueducts," <http://www.unrv.com/index.php?p=280>.

⁴ Charles E. Bennett, trans. 1925. *Sextus Julius Frontinus: The Aqueducts of Rome*, Leob edition, 1925.

⁵ Peter Aicher, *Watering Ancient Rome*, Nova Online, <http://www.pbs.org/wgbn/nova/lostempire/roman/watering.html>.

⁶ Wikipedia article "Roman aqueduct construction," under the GNU Free Documentation License. Also see <http://en.wikipedia.org/wiki>.

provided by the notable Roman administrator, Frontinus, “But the ancients laid the lines of their aqueducts at a lower elevation, either because they had not yet nicely worked out the art of leveling, or because they purposely sunk their aqueducts in the ground, in order that they might not easily be cut by the enemy, since frequent wars were still waged with the Italians.” It is believed by archeologists that the reason was not a lack of understanding of the leveling process but rather that they understood the relevance of placing these structures underground as a method of protecting their fresh water from external threats. During this period of early expansion, ancient Rome had many enemies and an above ground aqueduct would be a desirable and tempting target for the Italian tribes surrounding the city.⁷

There were three main advantages for building the aqueducts underground: (1) to conceal and to protect them from enemies; (2) to provide an additional level of protection from erosion and deterioration; and (3) to be less disruptive to life above ground. The primary disadvantage of an underground aqueduct system was the non-trivial difficulties associated with maintaining and inspecting the system. There was one other non-tangible disadvantage in the eyes of the proud Romans: placing these grand architectural works underground and out of sight deprived them of the opportunity to openly show the greatness and superiority of Rome. So how did the engineering requirements necessary to protect these structures evolve to see more sections of newer aqueducts rise from underground into the heavens, much to the pleasure of the common Roman and public ruler?

Rome’s Perception of Homeland Security Risks

In my opinion, it was both the advancement of technology and the change in how the Romans perceived risk that would drive more sections of the aqueducts⁸ above ground with magnificent arcades⁹ that many of us have traveled great distances to behold (see Figure 2).

⁷ Al Schlaf, “Aqueducts of Rome Under Augustus”, 2000, http://ancienthistory.about.com/library/bl/uc_schlaf1.htm.

⁸ The majority of most aqueducts were constructed below ground.

⁹ See glossary for definition.



Figure 2. Aqueduct design changed to include more above ground sections, hence becoming a more vulnerable infrastructure to security threats.

Let us now look at how the Romans perceived those risks, or more specifically, the threats to their homeland. In the early days of Rome, they were carving their existence out of the tribal landscape that comprised ancient Italy, so consequently, threats were close and constant.

This security situation changed over the next several hundred years as Rome’s dominance cut away at Italy and continued expanding until Rome’s territorial borders eventually encompassed the “known world.” Following the destruction of Carthage in 146 B.C., Rome was able to keep security threats outside the immediate Homeland (except for the insider threat posed by a slave revolt) and in those territories they considered the “frontier.” By ensuring the Homeland was secure, it allowed for innovation and civilization to flourish, and the city of Rome itself became a reflection of their growing power and achievement. Great public works and architectural wonders were being designed and erected and included important achievements like the archway and the dome.

Over time, Rome’s aqueducts began to change and better reflect her architectural greatness by incorporating the arcade to build more breathtaking above ground structures. The infrastructure changed from a hidden and purpose-built system that delivered an essential service into a “visible” symbol of greatness through the use of technology. The facade of achieving security is that it never lasts and that veneer results in the development of vulnerable systems and infrastructures. As we know, the reality of Rome’s security changed over time, and the frontier “barbarians” that had once been contained and dealt with by Roman legions, would in due course again threaten the city of Rome.

Eventually, the city of Rome became dependent on grain shipments from Egypt and the water supplied

by eleven aqueducts. As a result, invading forces found a vulnerable infrastructure to exploit and an effortless avenue to exert pressure. This ultimately dealt an unrecoverable blow to the capital of the western empire since the aqueduct's use of the above ground arcades made for an attractive target that was easily exploited. Several Germanic invasions were dealt with through military force. Each attempt could be repelled, but more successful Germanic attacks led to sieges where the enemies of Rome turned their sites on the visible and vulnerable Aqueducts. This action proved to be critical and Rome's necessary water supplies were disrupted. As the flow of water dwindled so did the hope of Rome's ability to repel the foreign invaders and recover the western empire. Ironically, the only aqueduct left in commission after these invasions was the Aqua Virgo which had been built underground to escape notice and be resistant to damage from Rome's ancient invaders. This underground aqueduct would supply water to Rome through the middle ages, leaving the city diminished to only sustain a fraction of its former population on the one aqueduct and remaining wells. (It is estimated that the city's population dropped from over a million to less than 30,000 through this time.) Eventually, several of the destroyed aqueducts would actually be repaired during the Renaissance to allow for restoration and growth of the city.

This story of destruction was repeated throughout the empire as adversaries attacked other Roman strongholds. Aqueducts were assaulted and disrupted around Cologne,⁹ Sardis, and other large Roman cities so the military, social, and economic impact of the aqueduct infrastructure's vulnerability to attack were far-reaching. One can only wonder if the hard lessons learned by later Romans would have sparked regrets for building more vulnerable aqueducts than their city's forefathers. The problem with this approach is recognized all too well by historians. By the time the Romans realized the real risks they faced it was far too late. Much like today, the consequences are not fathomable without a clearly demonstrated threat.

Aqueduct Security Lessons

Let's review some of the lessons derived from the story of Rome's aqueducts. One of the obvious truisms is that infrastructures can change from simple conveniences or enabling capabilities to critical necessities relatively quickly once they are put in place. In Rome's early history, the first aqueducts were a nice addition, improving a Romans' life and enabling the growth of the culture.

These early conveniences eventually became a necessity that both government and citizens depended upon. Their importance was directly tied to the security of the State and represented a common or public good.

An additional lesson revolves around how the Romans perceived risk and the societal impacts of realized risks. The aqueduct story that evolved over a period of almost 600 years demonstrates the life-cycle impacts of risk decisions (see Figure 3). The first and longest lasting aqueduct was built at a time where security risk was much easier to perceive and therefore mitigations were built into the design. In essence, security mattered to early Romans. Later aqueducts would be built in a time when the Romans no longer feared invasions since the barbarians were being held at bay thousands of miles away in the "frontier". The reduced sensitivity to security risk resulted in design modifications and the use of more vulnerable, however efficient and appealing, design choices. Modern day engineers should learn from this example and draw from it the understanding that design decisions should anticipate changing environmental and system factors including security. We must anticipate different circumstances because perceptions often lag reality and it can be disadvantageous and costly to weigh your options or implement changes only after security threats become too great to ignore. Built-in security is cheaper and more effective than trying to retrofit it after the system has already been placed into operation. Once the last brick has been placed, infrastructure design decisions have been "cast in stone" and like the aqueducts, typically built to last and hence, not easily changed or replaced.

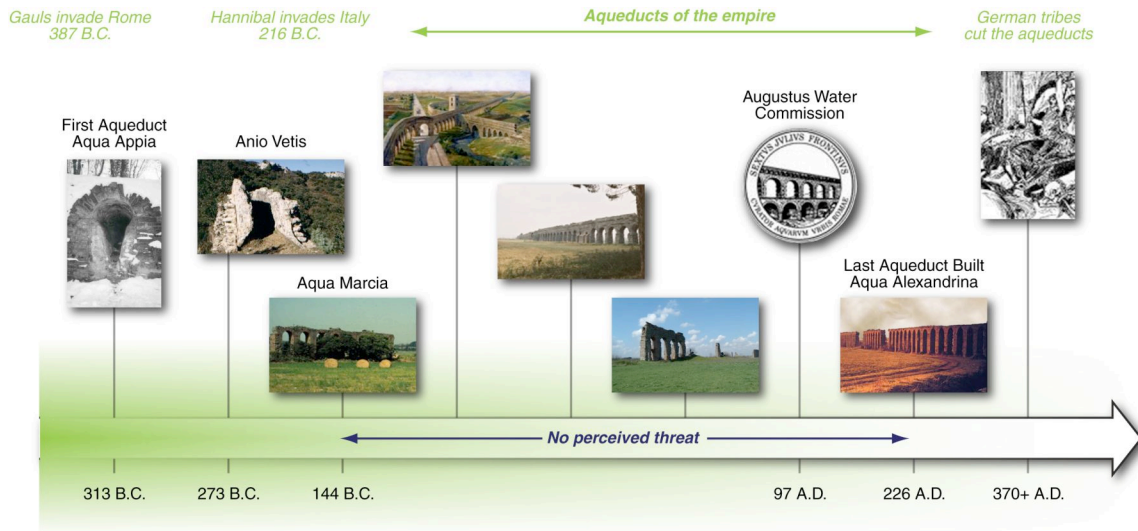


Figure 3. Changes in both homeland security and aqueduct design and construction.

The final lesson for those in government roles is that regulations or legislative requirements don't necessarily guarantee security. Simple requirements that don't align to consequential threats or offer protection may instead result in a false sense of security. It is difficult to mandate protections and safeguards, especially when the original design and existing infrastructure contains inherent vulnerabilities or weaknesses. The Roman Emperor passed edicts or laws to safeguard the aqueducts, but there are few indications that this was followed up with investments or action.

We can summarize these lessons into the following:

- Infrastructures are critical to the security of a state and represent a common good.
- Infrastructures are built to last and are seldom replaced.
- Incorporating new technology can introduce vulnerabilities.
- Security in the design is directly tied to how designers perceive security risk.
- Perceived safety and security dulls our senses.
- Many security risk decisions do not account for the life cycle of a system or infrastructure.
- Regulations and mandates with out investment and action do not guarantee security.

Ancient to Modern Infrastructure

Observing how Rome built, maintained, and protected the infrastructures that provided essential services to the people of its empire has historical value. Can we apply these lessons to the challenges facing America? Can we draw relevant parallels between the Roman aqueducts and our modern

critical infrastructures? Again, I believe the answer to both questions is "Yes". I will now examine how these lessons might help us understand the risks associated with our modern day infrastructures.

Experts acknowledge that one of the major issues defining the modern U.S. infrastructure protection challenge concerns the division of ownership between public and private responsibilities and resources. Rome experienced the same challenge with essential public services being developed in part by the State and typically turned over to private organizations and entities for their stewardship. In America, over 80 percent of the nation's critical infrastructure is owned or managed by private organizations.¹⁰ The balance of private interest and public good is at the very core of any critical infrastructure protection decisions. During later periods of the Empire, Romans provided for legal safeguards, but unlike past generations, did not go so far as to make investments and did not mandate security requirements into the design and operation of the aqueducts. The analogous question for us is: How involved and responsible should the State be in the security of the system?

To focus our comparison it might be most useful to choose one specific example of a modern infrastructure and draw the necessary parallels related to infrastructure protection. Power grids are a contemporary equivalent; however, the lessons can be applied more generally to protecting various other

¹⁰ GAO Report to the Committee on Energy and Commerce, House of Representatives, "Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors," February 2003.

critical infrastructures (see Figure 4). Much like Water to the Romans, it is easy to argue that cheap and abundant electric power is required to enable growth and support a large and prosperous population. If Rome needed access to water, then it can be said that America needs access to energy to be a successful world power. We can compare both similarities and differences in the infrastructures and security challenges we face today.



Figure 4. Modern electric infrastructure.

Similarities

Let's begin by looking at the infrastructures we are comparing. Aqueducts and power grids are similar in their need to move products (water and electricity) from sources across long distances to consumers. The aqueduct system is made up of sources (comprised of infiltration galleries built into rivers, springs, and lakes), transmission systems (comprised of chutes, settling tanks, tunnels, shafts, covered trenches, arcades, bridges, inverted siphons, and substruction), distribution systems (comprised of basins, towers, and lead pipes), and consumers (comprised of residences and industrial customers). The power system is also made up of sources (comprised of generation facilities such as coal plants, hydroelectric projects, nuclear plants, wind farms, etc.), transmission systems (comprised of substations, towers, control centers, Supervisory Control And Data Acquisition (SCADA), and power lines), distribution systems (comprised of substations, towers, control centers, SCADA, and power lines) and consumers or loads (comprised of residences and industrial customers).

They both share long expected life cycles. Some aqueducts lasted thousand of years while others only lasted hundreds of years after being destroyed prematurely by attackers. To this day, the basic concept of the aqueduct remains the preferred way to convey large volumes of water over great distances and elevation changes. The electric grid also remains largely unchanged, and the nations' reliance on this

infrastructure has grown in importance since its inception. Many power systems around the country rely on components that were a part of the originally installed system. For example, there are power lines in operation today that are over 88 years old.

There are two primary and important differences between water and electricity. The first is that water is tapped into (exists in a useable form), whereas electricity needs to be produced by converting energy from one form to another (referred to as power generation). The other important difference represents the greatest constraint facing our power infrastructure. Water can be stored; Electricity for the most part cannot. Electric power is consumed almost instantly after it is produced. The inability to store electricity of any significant volume adds an additional constraint on the system. An aqueduct that is disrupted will have an immediate impact, but the consequences can be offset, at least temporarily, by water stored in holding tanks or in the portion of the remaining system. Disrupting the power system will result in an immediate loss of electricity and can only be offset on a miniature scale by the use of batteries in very small devices or by relying on local backup power generation.

If we measure impacts and compare system functions, it is fair to say that the electric power grid is the modern world's equivalent to the ancient world's aqueducts. The comparison proves more valuable when we look at the similarities and differences in infrastructure security. The most obvious similarity has to do with the relative importance of the ancient Roman aqueducts as compared to America's modern power system. Both infrastructures are vital to each state's security and economic strength. A massive disruption of the U.S. power system would result in equally devastating consequences as the loss of Rome's aqueducts to foreign invaders.

Another more disturbing similarity has to do with society's perception of risk during the design and construction of the infrastructure. Much like Rome during its later period, the U.S. power system enjoyed a high-level of perceived homeland security prior to September 11, 2001. The relatively low perceived security risk has translated into few protections being deployed in the field and very little security designed into the actual systems. Electric grid participants haven't been completely naïve to the potential security risks and use a variety of approaches to protect the power grid including transmission planning, backup control centers, fences, security cameras, etc. When I served as the Chief Security

Officer at a major U.S. utility, it was apparent the infrastructure's physical components were inherently vulnerable to significant attacks. This can also be said of the use of information technology to help control and manage the electric grid. Some believe that vulnerabilities in this technological underbelly of the power grid should receive greater national attention due to the ability of cyber-attackers to exploit resident vulnerabilities from afar and in a scalable fashion.

Where the Romans incorporated new construction methods, specifically the use of the arch and arcade into the aqueduct, the power grid has used analog and digital technology to enhance control, provide data, and protect the system. These protections and control systems have allowed infrastructure owners and operators to more efficiently manage the power system by overcoming the challenges of scale, distance, and time. Both the Roman aqueduct and our power infrastructure began as improvements to how people lived, and later evolved into the necessities of life. This is also true of computerized control systems. Many of the processes controlled by computers and remotely networked systems have advanced to the point where they could no longer operate very long without that function.

The use of technology has resulted in more reliable power with a reduced need for manpower and resources. Cyber technology provides everyone with immediate global reach and exponential decreases in the constraints of time, distance, and power required. So while technology adoption has provided efficiencies it also has limits and challenges. As the arch and above-ground aqueduct construction introduced vulnerabilities, the use of information technology in the power grid has also resulted in weaknesses throughout the national electric grid infrastructure. These vulnerabilities allow cyber-adversaries to attack the infrastructure without the need to be in close physical proximity. In the ancient Roman context, this open access is like lowering the defenses of the Rome aqueducts to any "barbarian" living on the frontier of the empire. The proposition of "have axe, will travel" is one thing, but "have computer, will connect" is entirely different.

Cyber threats become more of a concern as cyber attacks can now easily rival the consequences of physical attacks. Recent research has demonstrated that cyber attacks can have physical consequences, and as a result, the Department of Defense (DoD) is considering an experiment using the application of cyber-force. In the DoD's mind, this question has already been answered. Jeffrey R. Cooper stated,

"Although attacks in the cybersphere do not involve the use of physical weapons, their destructive impacts, physical and otherwise, may be no less lethal to society."¹¹

In contemporary cyberspace, threats have been motivated by criminal activities, individual thrill-seekers, and cyber-activists. However, it is clear that military adversaries and trans-national threat actors are already considering or developing the use of cyber attacks to strike at nations with superior conventional military capabilities.¹² The capabilities available to the average human with a computer and an Internet connection are staggering. So much so that many have warned of a gathering storm that could disrupt many of the systems that our society relies upon. Clifford Lau, Chair of IEEE-USA's Research and Development Policy Committee has been quoted as saying, "The country's problem with cyber security is very serious and it is going to get worse in the next five years before it gets any better. I would say the situation not only is alarming, but it is almost out of control."¹³

Recent no-warning cyber attacks on Estonian government web sites and online banking infrastructures demonstrate that cyber-capable state enemies can target military forces, government institutions, critical infrastructures, or commercial entities.¹⁴ According to McAfee's® annual global cyber trends study, there were more reported cases of cyber-attacks on critical national infrastructures (financial market, utility providers, air traffic control, etc.) in 2007 than in previous years.¹⁵

Another relevant similarity with ancient Rome concerns the changing threat environment facing

¹¹ Jeffrey R. Cooper, "Another View of Information Warfare," in *The Information Revolution and National Security Strategy*, ed. Stuart J.D. Schwartzstein (Washington, DC: The Center for Strategic and International Studies, 1996), 122.

¹² John A. Serabian, Jr., Information Operations Issue Manager for the Central Intelligence Agency testifying before congress, Statement for the Record before the Joint Economic Committee on Cyber Threats and the U.S. Economy, 23 February 2000, Washington D.C.

¹³ IEEE-USA article, "United States Facing Cyber Security Crisis, Experts Tell Capitol Hill Briefing, As IEEE-USA Prepares New Position Statement," may be found at www.todaysengineer.org.

¹⁴ Rebecca Grant, Victory in Cyberspace, An Air Force Association Special Report, October 2007.

¹⁵ McAfee® Virtual Criminology Report, *Cybercrime: The Next Wave*, Annual Global Cyber Trends Study, 2007.

Rome's aqueducts and America's power system. After hundreds of years of peaceful life the ancient city of Rome was devastated by invading German tribes, and while we hope that the terrorism and cyber threats facing America represent only a temporary challenge to our way of life, we must be prepared for the alternative. The changes in our approach to security are dramatic enough to declare that a new reality exists with both physical threats to our homeland and cyber threats to our information systems. Much like the ancient Romans, peace has not prepared us well for the adversaries that have found their way to our real and virtual shores.

The final similarity has to do with aging of the respective infrastructures. Ancient Rome's aqueducts had become old and in need of constant repair. Disrepair, compounded by assaults from German invaders, exacerbated the maintenance problem. Our nation's power system is also old, requiring constant repairs and maintenance. These older systems are generally under more stress and show the same signs of brittleness that plagued ancient Rome. This has become one of our greatest challenges, and we have a very large legacy security problem to resolve. Many other countries are beginning to experience a wave of new economic growth and development requiring new infrastructure, which is putting them in the leadership position to drive lessons into change. The United States on the other hand is beginning to develop capabilities to identify how we can mitigate deficiencies within existing structures and systems and then compensate for the vulnerabilities inherent in their design (see Figure 5). We are also looking for opportunities to take a more proactive approach.



Figure 5. Can we add more security to the design?

Differences

These similarities are a harbinger of the necessity to re-evaluate the state of our nations' infrastructure and

its security. The differences between Rome's aqueducts and America's power grids don't offer any relief. It is actually the opposite. The differences between ancient Rome and the United States amplify the need to re-evaluate our approach to infrastructure protection. An important consideration is to simply decide who has authority over the protection of the Nation's infrastructure. In ancient Rome, it was the emperor that had clear authority with anything to do with security and the state. The public good represented by the aqueduct was well understood and the emperor and his governors were responsible for the protection of this common infrastructure. The U.S. power system has no single authority responsible for all parts of its security. In fact, there are few federal regulations and no single entity responsible for all the components of the U.S. power system. However, progress in reducing vulnerabilities is being made as there are several government agencies and initiatives making progress by partnering with industry to protect the nation's infrastructure.

The most significant difference between ancient Rome and the United States is found in the rapid pace of change in the security threats that face our modern infrastructure. It took hundreds of years for Rome's security situation to change, but the more recent rise of international terrorism has been measured in mere tens of years and the change in cyber threats can be frighteningly measured in individual months (see Figure 6). There are very real and unsettling implications to such a rapid change in the security

landscape. While it was difficult for Rome's perception of risk to catch up to reality over a period of centuries, we are challenged to re-think the risk situation in near real time as the ability of adversaries to employ devastating weapons grows almost daily. In the cyber realm, our power system's control technology faces a growing number of sophisticated technical threats that can remotely attack the systems from interconnected networks anywhere in the world. The means to remotely access SCADA and control systems, for valid operational reasons in many cases, have grown exponentially as disparate systems are increasingly connected through wired networks, modems, the Internet, and now wireless networks.

Another consideration that has provided a reason to stall our efforts to protect our vulnerable infrastructure is the question of whether likely

adversaries have taken notice (have they already?) of the nation's electric grid as a potential target? Ancient Rome's adversaries certainly took notice of the visible aqueducts. Most would aggressively argue that America's power systems are equally as important as the aqueducts were to Rome and are certainly as pervasive and visible. It is hard to conceive that once Germanic invaders understood the significance of the aqueducts to daily life in Rome that Roman authorities might question whether or not the aqueducts would be a potential target. We should ponder this question as well.

When we consider the physical threats to the nations' power systems, it's not necessary to look too deep to find examples of how a terrorist might target them.

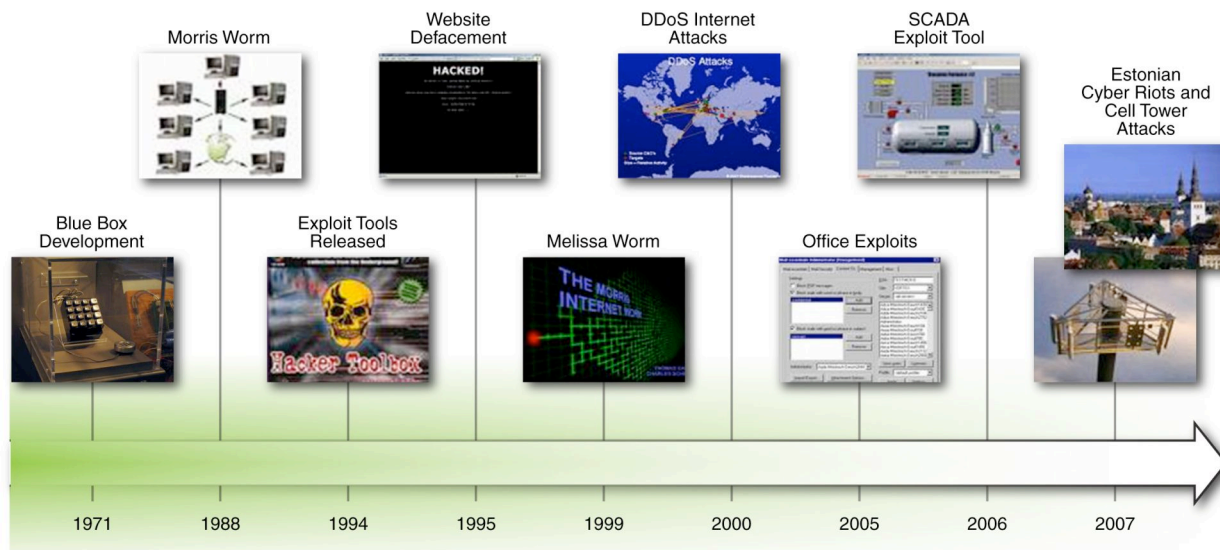


Figure 6. Rapid development of cyber threats.

Four important examples come to mind: (1) In 1996, the provincial Irish Republican Army was discovered plotting to bomb the London power grid; (2) In 2003, a Pakistani-born extremist was discovered working on a plot to blow up the power network serving Sydney, Australia; (3) In 2007, Islamic extremists were plotting to attack the Fort Dix Army Base and making plans to attack power system components to disrupt power and increase the effectiveness of their overall attack; and (4) On going successful attacks against local power systems has been reported in countries like Pakistan, Columbia, and Peru. These few examples, combined with news reports on the impacts of wide-scale blackouts, are enough for terrorist organizations to learn and adapt their strategies and tactics to recognize the consequences

associated with targeting power systems.

With respect to cyber threats as opposed to physical threats, while there is ample evidence of increases in cyber events associated with electric companies, it is less straightforward with relatively few public reports of direct attacks against electric grid control systems.

Another contrast from ancient to modern threats concerns the effort involved in exploiting the vulnerabilities found in both infrastructures. We know it took a relatively large Germanic invasion force to successfully attack and disrupt ancient Rome's complex aqueduct system.

However, unlike ancient Rome, it would take far fewer individuals to exploit the vulnerabilities found in today's power systems. While offering many advantages and improvements, technological advances invariably create adverse consequences. One of the world changing impacts of advanced technologies is that they often empower individuals or relatively small groups to wield the strength of what previously required many. I have termed this phenomenon "Micro-Force" that is the ability of a few to project power traditionally demonstrated by much larger or macro conventional forces. Micro Force describes the ability of a few to cause mass violence, major disruption, and destruction, as a force that has migrated downward from the nation-state to groups and even individuals. The best example of

this phenomenon is shown by the demonstrated ability of a small number of terrorists to effectively deliver over 7,000 kg of explosives to destroy targets clustered in several city blocks. In the 1940's, it required an entire U.S. Air Force heavy bomber wing to guarantee the destruction of targets covering the expanse of several city blocks. During the 1970's, the technical revolution enabled smaller formations of strike aircraft to accomplish the same goal. By the 2000's, one man in a truck has been able to demonstrate that same potential. To further illustrate this phenomenon we can compare the disparate level of effort between the military attack on Pearl Harbor and the terrorist attack on September 11th 2001 (see Figure 7).



Pearl Harbor Attack
December 7, 1941

- Thousands of men in uniform
- The most powerful carrier force assembled to date
 - 6 aircraft carriers / 28 ships
 - 420 embarked planes
 - 23 / 5 fleet / mini submarines
 - Significant resources used
 - Advanced weapons
- 2043 military / 68 civilian deaths
- Unobserved before the strike
- 2 hours of striking



Trade Center Attack
September 11, 2001

- 17 men in civilian clothes
- Terrorist operational cell
 - Resource use under \$1 million
 - Make-shift weapons
- 55 military / 2,938 civilian deaths
- Unobserved before the strike
- 1 hour of striking

Figure 7. Comparison of Macro to Micro Force.

Traditionally, the U.S. has feared other nation-states as security threats, but after September 11th, new security threats like al Qaeda have come into the nation's cross hairs. The British press reported an intelligence document circulated to the United Kingdom's MI5 counterintelligence service stated "We still believe [al Qaeda] will continue to seek opportunities for mass casualty attacks against soft

targets and key infrastructures."¹⁶ Al Qaeda represents one of the groups that have benefited from, and applied with drastic consequences, the Micro Force concept.

The Micro Force idea is a fundamental truism for adversaries in the cyber realm. By using computers, networks, and remote technology, it is possible for a

¹⁶ Sean Rayment, Intelligence Report Reassesses threat of Al Qaeda, London Sunday Telegraph, February 2007.

small number of individuals to conduct a widespread and damaging attack, while the implications of this technical shift are far reaching. How does a nation protect against small groups of individuals operating from remote and undistinguishable locations? Where the Romans had to field a superior military force to quash the threat posed to their aqueducts, what defenses do we need to field to protect the nations' critical infrastructure from cyber attacks? It is generally acknowledged that the nation is significantly less prepared to safeguard national assets from today's threats, so this is indeed a unique challenge for America.

The final difference between ancient Rome and the modern day concerns the physical and organizational complexity and scale of the two distinctly different yet similar infrastructures. The scale of Rome's aqueducts is impressive, but in comparison, the scale of the U.S. power system is utterly massive. There are over 157,000 miles of electric transmission lines, over 16,000 generators, and more than 3,000 distinct electric utilities with over 130,000,000 customers served by the U.S. power system.¹⁷ We enjoy some resilience from such a large system, but recent stress of limited large-scale generation and greater reliance on moving power over long

distances has eroded some of that resilience. Also, the sheer number of entities involved in providing power represents a significant challenge that is exacerbated by the dilemma of shared interest without responsibility or investment and further compounded by the split between public interest and private ownership.

Summary of Lessons to Apply

Given the rate of change, volume of change, and magnitude of exposure to security threats capable of negatively impacting our nation's critical infrastructures, it is more than prudent to re-evaluate our existing perceptions of risk.

It is historically unknown if the Romans understood the risk posed to their later above-ground Aqueduct systems and why they did not take action to mitigate the vulnerabilities that were eventually exploited (see Figure 8). It is possible that their decreased acknowledgement of the threat resulted in a commensurate decrease in resources required to take the necessary action. We know it to be true that merely passing laws or regulations with out investment and oversight does not effectively address risk.



Figure 8. Above ground aqueduct vulnerabilities were exploited by invading threats and suffered from erosion.

America must avoid this plight by taking a clear inventory of what is truly at stake and by making wise investment decisions to remove unacceptable risk. Successful private and public efforts to understand the problems and develop strategies to reduce the risk are underway. We would do well to learn from the mistakes of ancient Roman designers and better anticipate changing environmental risk factors. There is always the issue of how much risk is to be reduced and at what cost. The answers to these questions will have much to do with how we address the gap between public interest and private responsibility.

¹⁷ Energy Information Administration, U.S. Government official energy statistics, <http://www.eia.doe.gov/>

It is a challenge for people living in the present day to look at the past and recognize parallels between potentially similar negative outcomes. The story of ancient Rome's aqueducts is important and provides us with critical lessons to consider as we wrestle with the importance of protecting our own critical infrastructures. Rome's aqueducts, constructed during a time of peace, possessed vulnerabilities that would eventually be exploited by adversaries and resulted in serious and arguably disastrous consequences for the western empire. Recognizing the similarities and differences between the Roman aqueducts and the modern electric power grid gives us the chance to learn and evaluate how we should think about infrastructure protection. The changing threats that now challenge our homeland and infrastructures are in the process of being addressed, but more importantly, we need to identify what we can do to safeguard future infrastructure components. Unlike the Romans, we must not become an example for future civilizations to study. I leave you with a quote from Dwight D. Eisenhower, a man who distinguished himself during two of this nation's greatest national security challenges: "Neither a wise nor a brave man lies down on the tracks of history to wait for the train of the future to run over him."

References

Peter Aicher, *Watering Ancient Rome*, Nova Online, <http://www.pbs.org/wgbn/nova/lostempire/roman/watering.html>.

United Nations of Roma Victrix, "Aqueducts," <http://www.unrv.com/index.php?p=280>.

Charles E. Bennett, trans. 1925. *Sextus Julius Frontinus: The Aqueducts of Rome*, Leob edition, 1925.

Wikipedia article "Roman aqueduct construction", under the G.N. U. Free Documentation License. Please also see <http://en.wikipedia.org/wiki>.

Al Schlaf, "Aqueducts of Rome Under Augustus", 2000, http://ancienthistory.about.com/library/bl/uc_schlaf1.htm.

Thomas Ashby, "The Aqueducts of Ancient Rome," *The Journal of Roman Studies*, Vol. 26 part 2 (1936).

C. Vitruvius Pollio, *De Architectura*-Online: Perseus Text, Lacus Curtius, Frederick W. Shipley, *Agrippa's Building Activities in Rome*, Washington University Studies, 1935.

GAO Report to the Committee on Energy and Commerce, House of Representatives, "Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors," February 2003.

Smith's Dictionary of Greek and Roman Antiquities, Philip Smith, B.A., of the University of London, "Aqueductus", http://penelope.uchicago.edu/Thayer/E/Roman/Texts/secondary/SMIGRA*/Aquaeductus.html.

Hubert Chanson, "Some hydraulics of Roman Aqueducts. Myths, Fables, Realities. A Hydraulician's perspective," University of Queensland, Brisbane, Australia.

National Research Council, Making the Nation Safer: *The Role of Science and Technology in Countering Terrorism*, 2002 report.

Final Report. 2003. Final Report on the August 14, 2003 Blackout in the United States and Canada; Causes and Recommendations, U.S.-Canada Power System Outage Task Force, <http://www.nerc.com/~filez/blackout.html>.

U.S. Congress, Office of Technology Assessment, *Physical Vulnerabilities of Electric Systems to Natural Disasters and Sabotage*, June 1990, (Washington DC: U.S. Government Printing Office, June 1990) OTA-E-453, NIST order#PB90-253287.

National Intelligence Estimate, The Terrorist Threat to the US Homeland, National Intelligence Council, 2007.

Jeffrey R. Cooper, "Another View of Information Warfare," in *The Information Revolution and National Security Strategy*, ed. Stuart J.D. Schwartzstein (Washington, DC: The Center for Strategic and International Studies, 1996), 122.

John A. Serabian, Jr., Information Operations Issue Manager for the Central Intelligence Agency testifying before congress, Statement for the Record before the Joint Economic Committee on Cyber Threats and the U.S. Economy, 23 February 2000, Washington D.C.

Rebecca Grant, Victory in Cyberspace, An Air Force Association Special Report, October 2007.

McAfee® Virtual Criminology Report, *Cybercrime: The Next Wave*, Annual Global Cyber Trends Study, 2007.

Sean Rayment, Intelligence Report Reassesses threat of Al Qaeda, London Sunday Telegraph, February 2007.

Photo Credits

Figure 1. A portion of the Eifel aqueduct, Germany, built in AD 80, showing the calcium carbonate that accretes on the sides of the channel without regular maintenance, Wikipedia the free encyclopedia, <http://upload.wikimedia.org/wikipedia/commons/3/35/Eifelwasserleitung05.jpg>

Figures 3. And 6. are timelines built by the author using images from the public domain.

All other images were taken from the public domain or were paid for stock photographs.

Glossary

Aqueduct: From Wikipedia: An aqueduct is an artificial channel that is constructed to convey water from one location to another. The word is derived from the Latin aqua, "water," and ducere, "to lead."

Arch: From Wikipedia: An arch is a curved structure capable of [spanning](#) a space while supporting significant weight (e.g. a doorway in a stone [wall](#)). The arch appeared in [Mesopotamia](#), [Indus Valley civilization](#), [Egypt](#), [Assyria](#), [Etruria](#), and later refined in [Ancient Rome](#). The arch became an important technique in [cathedral](#) building and is still used today in some modern structures such as [bridges](#).

Arcade: From <http://www.britannica.com/eb/topic-507272/Roman-arcade>: An arcade with pilasters, or engaged columns attached to piers carrying an entablature, is known as a Roman arcade. During the late empire this was replaced by arches that rested on the capitals of a row of columns, a style that was standard in the Romanesque and Gothic periods and that was revived and widely used during the Renaissance.

Acknowledgements

This work was supported through funding provided by the U.S. Department of Energy to Idaho National Laboratory, operated by Battelle Energy Alliance, LLC, under DOE Idaho Operations Office Contract DE-AC07-05ID14517. Thanks also to Mark Weatherford, Chief Information Security Officer for the State of Colorado for his contributions and Scott Swartz, Control Systems Security Program Manager, Naval Surface Warfare Center – Dahlgren.

U.S. Department of Energy Disclaimer

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions expressed herein are those of the author alone and do not reflect the official policy or position of the Idaho National Laboratory, the U.S. Government, or the Department of Energy.