The Future of Digital Forensics: Keynote Address of the First Chinese Conference on Digital Forensics

Fred Cohen[1]

Abstract: This paper discusses the state of the art in digital forensics, where we want to go and how we will get there, and things to look out for along the way.

Key words: future; digital forensics; the state of the art

1. The state of the art and what we are missing

Understanding the future is generally helped by understanding the present. The present state of the art is under ongoing examination, and in an effort to keep an updated reflection of that state available, authors periodically write summaries. One such summary is the basis for the discussion of the art in this paper(Cohen, 2009). Figure 1 shows the items we discuss in the context of the overall structure.

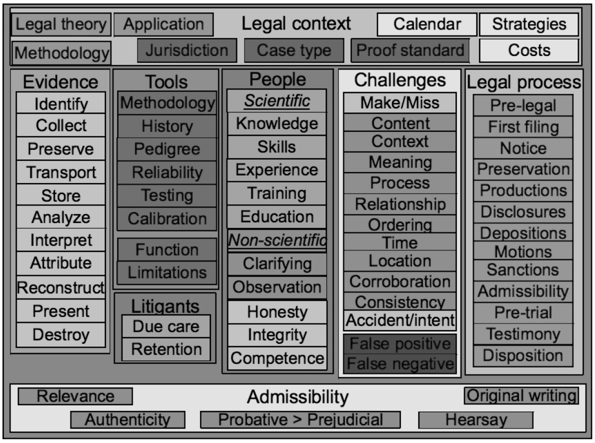

Figure 1 The structure used for discussion of the state of the art

[1] Fred Cohen is CEO of Fred Cohen Associates, CEO of Management Analytics, and President of California Sciences Institute.

1.1 We're not as dumb as they think we are

Many people think that forgery, alteration, or subversion of digital records is easy to do and will never be detected. But the art and science have progressed over the last several years to the point where this is no longer true. It is increasingly difficult to forge or alter digital records without those forgeries or alterations being readily detectable. At the same time, the "CSI phenomenon"[①] led to expectations far in excess of reality.

The reality is that, in the large, investigators and examiners can do some basic things quite well.

Identification of evidence, while problematic in many cases, regularly succeeds at readily identifying obvious direct sources, but redundant and related evidence is often overlooked, and courts often limit redundant information even though it is vital to evidence integrity checks.

Collection is well-defined and largely automated. Imaging media is excellent or nearly excellent for most media forms. Automated tools make forensically sound collection very easy, particularly for local permanent storage media. Tools like Drive Copy[②] reliably extract and copy disks directly in hardware with few human errors possible. Imaging over networks is not as good, but it is readily accepted in court when experts do the job properly.

Preservation is usually done very well. Live system forensics has made great progress gaining access to and imaging the operating state of machines while in action, network forensic collection has preservation capacity depending on the devices used to capture traffic and the bandwidth of the media, and preservation is readily verified later by the real-time introduction of cryptographic checksums into the hardware and software supporting the process.

Transport is fast, efficient and rarely a problem. While in the early days, disks left in patrol cars on a hot day were sometimes damaged with content lost. Today, most police forces have the necessary training and skills to transport digital evidence quite safely and reliably in most cases. In many cases today, transport over networks is used, and in these cases, while the full set of protections are often not applied, as a field, we certainly know how to do this reliably.

Storage can be done well and with integrity. Images are made and stored on disks or other media with cryptographic checksums of portions and/or the entirety. They are readily duplicated in pertinent parts, and in proper storage containers and lockups, with adequate chain of custody tracking, evidence can be well preserved for the time frames required for trial.

[①] *Crime Scene Investigation* is a popular television show that has produced an impression in members of juries that the state of the art is far beyond what it is in practice. The result is that the expectation of digital evidence is far greater than the reality commonly available today, and disappointed juries that rule on the basis of a lack of as much and definitive evidence as they have come to expect from CSI.

[②] MyKey technologies produces and holds the patent on this technology, however, there are also many other products that compete in this market.

1.2 We're not as smart as we think we are

There are, however, many areas in which experts commonly testify without the adequate knowledge to truly claim what they are claiming or understand the limitations on those claims.

Analysis is complicated and poorly understood. Much of the recent and current research is in this area. While many algorithms exist, the bases for most of these algorithms relative to a theory of digital systems are limited. For example, trace typing is problematic in that we only type traces based on assumptions of their type, and even then, largely ignore many of the potential inconsistencies or alternative hypotheses that may be applied. Embedded content, such as steganography, is largely ignored. Even simple searches miss many results, such as Hypenated and missspellled words, words spread across non-continuous blocks, and different character sets and representations.

Interpretation is often just plain wrong. For example, EnCase's interpretation of timestamps was incorrect in a legal matter where the time zones were critical and it claimed a wrong time and zone (United States v. Bayly, *et al.*, 2004). This case also displayed ignoring multiple time stamps, choosing one over the others, and the user not showing underlying data and interpretation method to challenge it. In another example, interpretation by a so-called expert failed to meet the "smell test" when they erroneously asserted based on claims as measured against actual distances, that computers communicate faster than the speed of light (Rose v. Albritton, 2009). Claims in that case also asserted that forgery was simple, but an attempted forgery by that "expert" in that cases as a demonstration was easily detected as forged, while the records at issue were not detected as forged by the same analytical method.

Attribution in networks is usually good at level 1[1], but at levels 2[2], 3[3], and 4[4] (K. Narayanaswamy, 2004), it is only good when done by nation states, who rarely allow law enforcement access to such information. Examples of successful attribution through anonymizers, onion routing, and similar deceptive methods that diffuse and confuse trackback processes have been successful in limited cases. For example, in one recent case[5], attribution of forged postings through UseNet groups and of a party stealing attorney client privileged communications through an anonymizer were both successfully completed. This included the use of an automated analysis tool to pick 33 postings out of more than one million postings and uniquely associate them to a posting from a separate site through similarity analysis (Cohen, 2010). The anonymizer

[1] Level 1: the direct IP address that did it.

[2] Level 2: the indirect source, or where the person who did it was.

[3] Level 3: the person who did it.

[4] Level 4: the organization behind the person.

[5] Susan Polgar v. US Chess Federation, *et. al.* In the US District Court, Northern district of Texas, Lubbock Division, C. A. NO. 5-08CV0169-C, Sep 15, 2009.

service was defeated for attribution by financial, timing, address, and related records, and their fusion into a legal process caused the perpetrators to admit their identities as part of their attempt to defeat the attribution. Clearly, these are examples where automated mechanisms are required and only limited such mechanisms are widely available. Just as clearly, these are examples which automation alone is inadequate.

Questions like "Who launched the ××× worm?" are similarly solvable, in this case by infection backtracking to lead to identifying victim 0 and sourcing from there. There are few cases and experts where this level of effort is undertaken and expertise is available, but it can often be done with enough resourcing and access to enough relevant and available data. The challenge in this case is getting more in law enforcement who understand what can be done and how it can be done, and developing more automated methods to support these tasks.

Reconstruction is poorly understood and not adequately studied. As a result, it is expensive and hard to do well. It takes time because of inadequate underlying support, but it still happens from time to time. A counterexample from 2001 used manual reconstruction that showed claims of the prosecution to be unsupported by the facts. More recent automated reconstruction methods have been developed (unpublished), and automated reconstruction for attribution testing has produced demonstrable tests in situ for causal chains. These results include automated particularization to mechanisms and individualization via related records.

Presentation is problematic for many sorts of data. Even the simplest things are poorly presented in many cases, such as the text associated with message headers or the content of Word documents. But methods like Forensic Fonts(Cohen, 2010) are starting to be used to resolve these issues and provide simultaneous traceability and readable precise presentation. But this field has a long way to go, and is fundamental to examination if only because examiners use presentation to themselves in order to understand and examine evidence in all cases.

Destruction appears largely settled. We know what can and cannot be recovered in most cases. For example, recovery of overwritten areas of modern hard disk drives has been shown infeasible by both keyboard and laboratory attack according to the NIST 2006 review of hard disk wiping by overwriting(Guidelines for Media Sanitization, 2006).

Sandia studies of rapid destruction circa 2000 (unpublished) demonstrate that many methods are not very effective, and in many cases, shortcuts produce inadequate destruction. For example, the Chinese booth at the 2012 RSA conference demonstrated a set of destruction technologies that could readily be defeated by data recovered in a laboratory. While they may be suitable for most commercial uses, they are ineffective against a government or for very high valued content.

1.3 Our tools are limited and lacking

We lack a real scientific basis for most tools applied in digital forensics. While we notionally discuss issues of science, recent studies indicate that there is a lack of consensus in the digital forensics community surrounding the scientific principles(Cohen, Lowrie, & Preston, 2011), and this has subsequently been tracked to issues related to common language and publication standards(Cohen, 2012). The methodologies we currently use as a field limit what we can do and understand regarding analysis, interpretation, attribution, reconstruction. While commercial tools typically lack the sorts of pedigree and quality of high grade software, trusted systems and trusted development, proof of correctness, well understood algorithms, well tested software, reliable operations, output tied to source data, and similar methods are largely unused in this arena. Methodologies for calibration are just emerging, and in many cases, we don't even have well defined functions and specified limitations, at least in commercial products.

1.4 People issues

Almost all law enforcement officials I have encountered in this field are honest and have high integrity. Only very few cases have been identified where this is not true. The "real" experts are honest and have high integrity in all areas and cases I have seen. But, at least in the US, experts for hire exist, and are often of low quality and will say anything for enough money. While courts often identify these "experts" as not credible, they also often end up admitted as experts and testify in ways that harm both the cause of justice and the credibility and precedent required for long-term justice to be served.

Competence is a different issue. It stems from knowledge, skills, experience, training, and education, and without an adequate educational system and scientific basis, it is unattainable for the massive challenges facing global law enforcement.

At the national security level, there are many very smart and dedicated people with extremes in knowledge and skills, excellent experience over many years, and strong training and operations. While there is still limited education and more tradecraft than science, national security mechanisms are far advanced from those of law enforcement.

The legal system, and more particularly, law enforcement is normally given short shrift. Much of the national security tradecraft is not available to law enforcement because of secrecy. Revealing these secrets may reveal too much information and endanger national security, but at the same time, national security is imperiled when the system of justice leads to unjust results. This tradeoff is called the "equities" problem, and underlies many of the challenges faced by normal investigations in the legal system.

Knowledge is limited by lacking of funding for science. While this is related to equities issues, it may be changing. There is more push for science and engineering today in this area, but still a lack of funding and recognition. For example, "The Physics of Digital Information"① is a chapter on the fundamental science underlying digital forensics, but it was developed in spare time over a period of more than 10 years, and had no funding. The area will continue to lack

① See http://infophys.com.

funding in the US as those funding long-term research in this area have a focus away from this approach.

Skills tend to come through practice and training, and tend to be reasonably good in areas with well-developed technology. Training on commercial technology is good, largely because it fits the business model of the technology providers, who may make more from training than for their tools.

Experience is limited because of rapid changes in information technology. For example, cloud computing, mobile devices, pad technology, and other similar breakthroughs in widely used technologies are almost always ahead of the capacity of forensics and law enforcement.

Education is also severely lacking. For example, our program at California Sciences Institute was the first US PhD. Program in digital forensics, and is years away from producing its first doctoral graduate.

The challenges of a lack of adequate scientific basis for much of the field and the lack of progress in these areas is largely supported by recent reports in the US justice system, and these issues are broadly reflected on a global basis(National Institute of Justice & National Research Council, 2012).

1.5 Management science is lacking

For many in the technical fields, management science is seen as an oxymoron. But there is a clear need and lack of attention to the issue of how to match limited resources to high demand in law enforcement in general, and in digital forensics in particular.

Case management is in its very early stages. The Hong Kong Police Force and their joint university research is the best example of starting in this line of research(Kwan, Chow, Law, & Lai, 2008).

Their efforts in forming Bayesian models of evidence needed to support cases, adding in prosecution history to identify needed evidence, identification of what evidence to seek first at all, earlier cut-off of bad cases, clearing the innocent, earlier determination of good cases (likely guilty), and earlier cut-off when enough evidence is found, demonstrate more than just cost effectiveness. They support the rights of the innocent and the public good. More efforts in this arena are likely to have a substantial positive effect.

Legal context drives the management of cases. But legal theories are rarely codified into frameworks. While there are counterexamples in the charting of laws by law enforcement to make cases and explain them to juries, theoretical work largely ignores case experience. Those working on cases rarely do theory and vice versa. The lack of scientific methodologies to base work on means that you cannot properly apply methodology you don’t have.

Lack of models for optimization leads to a lack of automation to support processes and calendar. Except for the HKPF example cited earlier, no real efforts in strategy and cost have been identified, and the tradeoffs of jurisdiction, case type, and standards of proof remain an amorphous judgement call by individuals.

Jurisdictional issues are obviously well understood. Each has a long history of jurisprudence, including laws, regulations and case law. Precedent in all but the international realm tends to rule, and even there, the history of relationship tends to dictate likely outcomes. A lot of cooperation exists on a global basis for hunting perpetrators, and those that do not cooperate are sanctioned in various ways. But these issues are largely limited by political will, which supports some activities and not others. This ultimately hinges upon global treaties and precedent, and that will take a while. Proof standards may be very tricky as there is a lot of judgement involved. Historical data is needed, and again HKPF leads the efforts to gather and apply such information. Limited attempts at case management help to keep track of cases and the large amounts of related information, but these technologies are information-support only, and generally do not help the decision-maker.

2. Where we want to go and how we will get there

Most people of the world and most law enforcement largely share the same views on what a system of justice should hope to achieve. A future vision outlined here is commensurate with those almost universal principles of a system of justice. But they may not be compatible with all political systems, and justice tends to work against those who prefer injustice that favors them.

2.1 A future vision

The future vision is well served by a list of goals:

- **Only criminals get arrested and prosecuted.** Ideally, those who are not guilty of crimes, regardless of the system that defines those crimes, are left alone by law enforcement, except to the extent that they are victims or witnesses of crimes, in which case they should be supported and helped.
- **Innocents are rarely investigated and never charged.** Nobody gains from the fruitless investigation of those who did nothing illegal. It wastes resources that could be better spent elsewhere, and it degrades trust and belief in the justice of the system.
- **Court cases are rock solid on a sound basis.** By the time a case gets to court, the evidence in support of the case should be overwhelming and clear, free of defects, and hard to question in any serious way.
- **Costs are low, danger to the public is low, and officers are safe.** Nobody wants to waste money or time, but it is worth the expense if it helps assure that officers and the public are safe. Officers should not need to take exceptional risks in order to enforce the law, and the public safety is, of course, one of the main goals of a system of justice.
- **Only the necessary information is gathered, processed, and used—and only within**

the legal strictures of jurisdictions. Missing relevant sources of evidence, whether exculpatory or inculpatory, should become rare, and challenges associated with jurisdictions and standards of proof should be resolved across the globe.

- **The evidence is overwhelming—and the courts agree.** While many cases today proceed on only the slimmest thread of evidence, and many criminals try to destroy or avoid creating the evidence that would convict them, the ideal future brings so much evidence to bear and in such a clear way that there is no serious doubt of the matter at hand.
- **Corruption is almost non-existent and easily detected.** While people are imperfect and some level of corruption is bound to remain in any human system, detecting corruption at all levels should be highly successful and the resulting prosecution of corrupt officials should act as a strong deterrent to future corruption.
- **The public has high confidence in the integrity and fairness of the system and it is transparently so.** All of the details reasonably necessary to believe in the integrity and fairness of the system should always be under public scrutiny and the public should be able to come and verify it, if desired, on a personal basis. The system should be so transparent and clear that those who question it with any rational basis should be readily satisfied, and those with purely irrational views should be readily exposed as such to the public at large, with the basis for that exposition readily clears for all to see.
- **Detection, arrest, prosecution, and punishment are sure, fast, and just, and everyone knows it.** This has long been claimed to be the best deterrent to crime. If everyone knows that crime is detected and punished all the time, those who commit crimes only do it a small number of times over a short period, and those who do not commit crimes need not fear substantially from those who do.

2.2 Achieving the future vision

Achieving this future vision is within the grasp of human society. There are no technical challenges that cannot be met in this arena, given an adequately knowledgeable and skilled team of specialists properly supported and led. None of the technical challenges are so novel or extreme that they require breakthroughs in mathematics or science, and there are adequate fundamental capabilities available today to engineer the sorts of capabilities discussed here. No doubt some may come more easily and quickly than others, but they are all attainable. The nature of the underlying challenge then is not technical in nature, although there are many technical challenges ahead. The things that might prevent this future from being realized are resourcing and leadership.

2.2.1 Only criminals get arrested and prosecuted

Key factors include the reliability[1] of evidence and attribution of actions to actors (at 4 all levels). I maintain that this is adequate in an otherwise just system, and that it is achievable from where we start today. Reliability can be established by systematic production and analysis of redundancy, while attribution can be attained by increased sensors and analysis regimes built into the infrastructures and operational models of the systems of the world. To paraphrase General Alexander, unlike the other domains of warfare, the information domain is one made by people, and people can rebuild it to meet the requirements of our civilization.

2.2.2 Innocents are rarely investigated and never charged

This is an optimization issue closely related to HKPF efforts previously cited. If we understand what evidence makes a case, we may rapidly identify, collect, and analyze only the necessary evidence to rule out suspects as soon as possible. Near-real-time examination of relevant records for classes of acts is already feasible in some cases. While there is a long way to go, the development of standards of practice and advancement of the relevant fields will increasingly reduce errors and omissions. With added reliability comes added assurance against false positives and negatives.

2.2.3 Court cases are rock solid on a sound basis

This is a matter of doing the science necessary to provide the basis for everything produced regarding the forensic evidence. While we largely lack such scientific efforts today, it is only a matter of emphasis that will keep the field from rapid advancement. The basis for much of this science already exists, but we need to learn to apply it, study and teach it well, and present it clearly.

2.2.4 Only the necessary information is gathered, processed, and used—and only within the legal strictures of jurisdictions

See the optimization issues discussed above.

2.2.5 The evidence is overwhelming—and the courts agree

This requires systematic collection, retention, analysis, and review, and tracking of legal decisions for what is and is not acceptable. In some sense, this is very similar to the efforts of the HKPF but on a far greater scale. While automation has crept into selective areas of digital forensics, it is almost all in the collection, preservation, and search realm. A substantial expansion into the entire range of issues is necessary in order to advance the field in a big way.

[1] Reliability: From Diplomatics, the record reflects the reality it purports.

2.2.6 Costs are low, danger to the public is low, and officers are safe

Automation on a large scale reduces cost in the long run, but over the short run, large-scale investment in research, development, and deployment is necessary in order to achieve the long-term goal.

Optimizations discussed earlier reduce costs, and for some classes of crimes, automated ongoing analysis may rapidly detect possible crimes, identify and collect just the right evidence, preserve it, do analysis, attribute acts to actors, and present the case for human review. Some such mechanisms already exist for some classes of activities in some environments, but at a larger scale, the challenges are far greater and there is a long way to go. As an example, in well controlled computing environments with low base rates of activities of import, indicators are already rapidly detected, automatically analyzed, and presented to investigators in a form suitable to legal use.

Operational security is a key to effective digital officer safety. This is a well-established area with a lot of sound practice, but it is largely tradecraft and not widely practiced. The Federal Law Enforcement Training Center (FLETC) in the US, and Kevin Manson in particular, did an outstanding job of building this into the training program. At a basic level, this requires that risks to the officers be considered and traded off against other equities. If criminals can do attribution as well as law enforcement, then criminals can find the officers as well as officers can find the criminals. Unless there is a differential in capabilities, this makes safe undercover work infeasible. Thus some level of secrecy will be necessary during investigations.

2.2.7 Corruption is almost non-existent and easily detected

Redundant records provide the means of detecting falsifications of records today. The technology for automating this at large scale is now being tested and deployed in select environments. This is the future basis for questioned documents examination that will roll into the legal system as standard practice over time. The leverage is shifting to where detecting subversion is far easier and more reliable than forgeries or deceptions. While not all corruption involves subversions, much of it does, and these advancements will go a long way to rooting out insider effects.

2.2.8 The days of easy/feasible forgeries are over

In case after case, where adequate expertise is applied, forgeries are detected and responsible parties punished. The myth of forgery without detection still persists, but the reality does not. The challenge is getting these changes into the legal system and the digital forensics process.

2.2.9 The public has high confidence in the integrity and fairness of the system and it is transparently so

As the changes described above get integrated into the legal system, public confidence will grow, but only if we do it well. As much as possible, transparency must be achieved, and the press and public must know the reality of what works, how well, and why. The global academic community must be integrated into the public process and support the validity of the results in order for this to be successful, and global scientific consensus surrounding the science and methods must be broad and clear. The global educational and research system must support ongoing open science to build the global capacity and the science and arts involved.

2.2.10 Detection, arrest, prosecution, and punishment are sure, fast, and just, and everyone knows it

This will follow from all the rest.

2.2.11 But to achieve it, we need resources and support adequate to achieve it as a global goal

Nation states can only go so far on their own because of the global nature of crime and policing. If and as we fight against global crime, we will throw out the information age baby with the bathwater unless we can find ways to cooperate. Crime is global and globally organized—crime fighting must also be global or it will fail to meet the challenge.

2.2.12 Don't forget the civil cases

Legitimate civil disputes require similar capabilities to criminal cases, and indeed, often more resources applied by all sides for high valued civil matters than criminal cases. Different standards of proof and discovery requirements, few of the permanent infrastructures in place for civil matters, and far less repeatability are available in cases. Each is fairly unique. But civil justice is just as important as criminal justice. Confidence in a political system demands justice at all levels, from the petty thief through the corporate raider. Advancements in science and engineering require protection of intellectual property or investment will collapse. In addition, personal motives drive many innovators, and ego is as important as money, so we must learn to be scholarly and to give credit where due—attribution for those who advance the field is important to continuing advancement.

3. Things to look out for

While seeking to meet this future vision, we must be aware that with great opportunity comes great risk. Some things we need to look out for including those identified here. But this list is hardly comprehensive. One of the things we most need to do is strategic thinking and action based on that thinking. But this is an area where nobody seems willing to focus resources or attention. As a result, for now, as a field, digital forensics operates largely in a reactive mode, driven by events, and never ahead of them.

3.1 The opportunity ahead

The opportunity of today starts with strategic thought and investment in key areas. It will not be inexpensive, nor will progress likely be as rapid as we might all wish. But failure to invest will bring yet another generation of crime without punishment, public dissent without recourse, and failures of law enforcement on a global basis against the very forces that ultimately become the threats of the future. Every major criminal organization of today was once a few individuals or a small group of rank armatures. It was the failure of the legal system to deal with the threat properly that drove its evolution into what we have today, and it will continue to evolve unless and until we get ahead of it.

3.2 Big brother and going too far

There has to be a balance between freedom and justice. While that balance varies in the global community, those seeking justice must be keenly aware of the need for freedom in order to gain prosperity.

Unlimited freedom leads to people unjustly taking advantage of others—a human rights issue we all face. But perfect justice at the cost of freedom guarantees that we will all be mediocre and society will stagnate. A balance must be struck and adapted over time.

In addition, any such system must recognize that people are not perfect, and neither are computers. Whatever we do will be imperfect because we are imperfect. But by striving to always improve, we will lift all boats. Resiliency and transparency are the main guarantors of justice, and a system that is to prosper must self-correct to support the will of the people without supporting the tyranny of the majority.

3.3 The equities issue

The balance between secrecy and justice must also be struck. While secrecy is normally an attack on justice, as we have seen, justice sometimes demands some level of secrecy for some period of time. We all recognize that secrets are necessary in a hostile world, even if we wish it wasn't a hostile world. We all recognize that justice is the solution to many of the problems of the world (both criminal and social justice), but we may disagree about the balance.

My personal view is that attack has been given too much of the resource in the information arena, and as a result, defenses suffer. The net effect is that crime is easy and rampant, justice is hard and hard to come by, and we need to seek a better balance of the equities toward justice.

3.4 Emerging times and the race

We are in a race today. It is a race against flash mobs, social media abuse, and cybernetic attacks on cybernetic critical infrastructures. And it is a race that will cause great suffering and injustice if the forces of justice fail to win it.

3.4.1 Flash mobs and instant forensics

Flash mobs today are faster than police. In London, flash mobs used social media to report on the presence and movement of police and thus the mobs were able to avoid police, while the police were unable to take advantage of the technology to detect and get in front of the mobs. At the same time, the notion of instant forensics necessary in order to defeat flash mobs is well beyond the current notions of digital forensics. Rather, this is largely an intelligent function, and one that potentially leads down the road to oppression.

Somehow, police need to be able to get ahead of events as they happen, but the technology supporting this must also support attribution after the fact that those responsible for criminal acts are to be properly punished. The London subway bombings demonstrated the use of closed circuit television after the fact, as did the killing of a Palestinian in a Dubai hotel. But in both cases, deaths resulted before the police were able to get involved. On the other extreme, in the San Francisco area, the bay area rapid transit (BART) system shut down telephone service to all of its riders in order to counter attempts to use cellular technology in protest against a BART police killing. How and when to intervene in advance and how much resource to put into such an effort are key factors in deciding what the responsibility of police is and when and where it is appropriate to use what methods.

3.4.2 Social media and the information currency

Wiki-Leaks and the "information needs to be free" culture have led to an increased challenge on a global basis to the confidentiality of data. Independent actors exploiting weaknesses in information technology and soliciting insiders to do their dirty work have used deception and taken advantage of human weakness to gain access while using the commons of the Internet and propaganda methods to gain support and retain freedom while attacking every manner of authority, from companies to governments. Small groups have led the way in this arena, but the common perception and claim that they are David and Goliath struggles emerging from purely social media is just not the truth.

Insiders who violate their oaths of loyalty and turn on their families and their responsibilities commonly do so in the name of justice. But they also commonly produce greater injustice and fail to ever realize it. They are largely dupes of more agile and intelligent people who take advantage of them for ego gratification, money, and power and stature within specific communities.

Revolutions in the Middle East, while touted as the natural result of social media, are in fact led, in most cases, by well organized groups that worked over periods of years to achieve those revolutions and took advantage of tactical situations to achieve long-planned strategic goals. They can, potentially, organize to overthrow almost any government that creates the conditions for revolution by oppressing its people and/or denying them the things they clearly see as available to the rest of the world. For many years, there was a notion that the Soviet Union could be overthrown by dropping millions of small two-way radios into the population. The idea was that once they were able to understand the oppression they were living under and had the means to securely communicate, they would surely organize and revolt. This is the natural result of an oppressive government.

3.4.3 Steganography, cryptography, and Linux

These are, increasingly, the info-weapons of the day. Used by criminals since the beginning of communications technology, they have always been used to avoid or defeat law enforcement attempts to catch them. But the modern era has brought high quality free encryption to the masses with easy-to-use interfaces. Add steganography and global communications, and the result is covert communications at a scale never before met. Countering these methods required far greater understanding and technological assistance than has previously been available to law enforcement. Within the flexible and largely reprogrammable Linux environment, information hiding and altered function become within the preview of even the single actor who has good computer skills and a desire to learn. But there is also opportunity for government to apply these technologies for lower cost higher quality specialized mechanisms and systems. China is asserted to be developing its own versions of Linux, customized to meet its own needs, and other governments have done the same things for their needs.

While governments have long been developing methods to defeat such things, they occasionally get caught, largely because of human failures. But don't imagine that these technologies are unbeatable. They are in fact regularly defeated, just not as regularly be law enforcement as by intelligence organizations.

3.4.4 Cybernetic society and critical infrastructures

Cybernetics has been a field of study for a long time. It studies the use of feedback systems in control applications, and is increasingly a term used in a more generalized fashion to discuss "cyber space". But in the more restricted form of usage, these feedback systems form foundational elements of the critical control mechanisms associated with critical infrastructures.

As technology has advanced and the rush for automation has overtaken the thoughtful engineering of the past, less and less time has been taken to understand the nature of feedback systems and decisions have been made on increasingly large scales to increase risk while mitigating negative effects by actively altering systems over time to defend them. But in critical infrastructures and situations with serious negative consequences of failure, this is a very high stakes game that is being badly misplayed around the world.

Attack mechanisms like Stuxnet may be exploited against commonly used and interconnected systems to devastating effect. It is unclear that law enforcement will ever be able to help protect and defend the population against these sorts of events. If the attacks directly hit law enforcement systems, how do we continue? While most police organizations have redundant radios and similar communications capabilities, coordinated attack and defeating of police communications systems are clearly a risk to the public well-being. While at some level this becomes a national security issue, do we really expect police to investigate cybercrimes of this sort? If so, how exactly will this happen. The system specific knowledge and ability to track perpetrators over infrastructures stretches far beyond the current resourcing for most police agencies. It almost seems that a version of the SWAT teams used for physical events will become necessary for police, complete with new special weapons and tactics to defeat and catch the cyber criminals.

3.5 Research, education, law enforcement, and their integration

There are many things we know how to do well, and technically, there is a great deal we can do today. But most in law enforcement lack the knowledge, experience, training, education, and skills to work in the information arena. If we are to fight cybercrimes and apply digital forensics effectively, this must change. While the physical police actions we expect will still be vital, and interviews and interrogation will remain vital, the time is soon coming when much of the detective work associated with digital systems will need to be done by specialized experts in laboratory environments.

There is still a lot to learn, and few people have a lot of know-how. We need to share what we know as we learn more and turn this knowledge acquisition and sharing activity into a normal part of law enforcement, just as law enforcement has done in other arenas over the years. The rate of progress is currently limited by who is resourced to what level for what purpose. Resourcing must change if progress is to be made at the pace of change.

Partnership is the best way forward that I know of.

University researchers working with real world examiners and students are one of the best approaches to partnerships we have found to date. Advancement of the state of the art calls for high quality research over time, and universities have historically been the ones to do this. But today's educational system requires some level of expertise from industry, and the most advanced researchers we have identified are insufficiently supported by universities alone.

Solutions to current challenges will likely come from a short-term investment in the best and the brightest building strategies and carrying those strategies out by leading research teams across the world. Universities and their students should be engaged in this process and cooperation with law enforcement worldwide should be used to lead toward solutions to the right problems. Building the capacity for future workforce and research is the only way to win the current race.

In the end, we need a positive feedback system to grow justice and knowledge both together. I believe that universities worming hand in hand with law enforcement will help to form that positive feedback system and build a just society from the ground up.

4. Summary, conclusions, and further work

As a field, digital forensics is weak in many areas. But there are some areas of strength we can build on. A lot of progress has been made lately, and even though much of it is not yet available in the open market and as a science it is not openly and adequately supported, there is a tremendous opportunity for rapid progress and a tremendous need for such progress.

There is too little resourcing today and it is largely directed in the wrong ways to achieve what we all want to achieve. A future vision is realizable in parts and over time, and it may be achieved in pieces where it is prioritized. But a far better approach, and one that is far more likely to win the race against crime and put forensics on a firm standing for the information age, requires that the best and brightest in the field be funded properly and used as seed corn to build the future stock of expertise and researchers to get ahead and stay ahead.

The future of justice also demands open global cooperation. In the words of two great commentators on justice and the human condition:

"Sunlight is said to be the best of disinfectants."——Justice Lewis Brandeis

"Injustice anywhere is a threat to justice everywhere."——Martin Luther King

References:

[1] Cohen, F. Digital Forensic Evidence Examination[M]. Fred Cohen & Associates, 2009.

[2] United States v. Bayly, et. al., United States District Court, Southern District of Texas, Case No.: H-03-363. Oct. 25, 2004.

[3] Rose v. Albritton, Superior Court of the City and County of San Francisco, Case No.: FDV-09-806677, July 14, 2009.

[4] K. Narayanaswamy. Survey/Analysis of Levels I, II, and III Attack Attribution Techniques[M]. Cs3, Inc., April 27, 2004.

[5] Cohen, F. Attribution of Messages to Sources in Digital Forensics Cases[J]. HICSS-43, Jan 7, 2010.

[6] Cohen, F. Fonts for Forensics[J]. IEEE SADFE, May 19, 2010.

[7] Guidelines for Media Sanitization[J]. NIST Special Publication, Sept. 2006.

[8] Cohen, F., Lowrie, J., & Preston, C. The State of the Science of Digital Evidence Examination[J]. Seventh IFIP WG 11. 9 International Conference on Digital Forensics, Jan.

30, 2011.

[9]Cohen, F. Update on the State of the Science of Digital Evidence Examination[J]. Conference on Digital Forensics, Security, and Law, May 29-31, 2012.

[10] National Institute of Justice, & National Research Council. Strengthening Forensic Science in the United States: A Path Forward[M]. BiblioGov, 2012.

[11] Kwan, M., Chow, K. P., Law, F., & Lai, P. Reasoning about Evidence Using Bayesian Networks[J]. Advances in Digital Forensics, 2008(4): 141-155.