READING & WRITING ASSIGNMENTS

# Cybersecurity

*One theme - four different reading options.*

---

## In this packet (suggested pairings):

- **AP Computer Science Principles**
  The Map That Gave Away the War (Location Data)
- **AP Computer Science A**
  An Army of Baby Monitors (Mirai Botnet)
- **Cybersecurity**
  The Weapon That Got Away (WannaCry)
- **Independent Study**
  Pay or Bleed (Ransomware)

Each assignment shares the same spine: a specific story, the broader concept, at least four of your own sources, tiered questions, and a prepared for/against debate.

READING & WRITING ASSIGNMENT

# The Map That Gave Away the War

*Location Data, Metadata, and Accidental Exposure*

## The Story That Started This

In the fall of 2024, I started training for the 2025 Cherry Blossom Ten-Mile Run in Washington, D.C. I'd never run more than two miles at a stretch, so I went looking for a training plan and a community to keep me going. A few friends pointed me to **Strava**, an app where you log your runs and see everyone else's. I loved it. What I didn't stop to think about was that every run I logged also quietly recorded where I live, the routes I take, and when I take them - and shared a good deal of it with people I'd never met.

In January 2018, a 20-year-old university student named Nathan Ruser was scrolling through a map published by the fitness app **Strava**. The company had released a global "heatmap" - a glowing picture built from three trillion GPS points logged by its users out jogging and cycling. In cities it just looked like a pretty tangle of streets. But out in the deserts of Syria, Iraq, and Afghanistan, where almost no locals use fitness trackers, the only people running in neat loops were **soldiers**.

Those loops lit up the map. The heatmap quietly revealed the perimeters of secret military bases, the supply routes between them, and the daily patrol patterns of the troops inside - even a suspected CIA base in Somalia and a missile-defense site in Yemen. Nobody hacked anything. No password was stolen. Soldiers just went for a run with their watches on, and an app helpfully published where. The U.S. military had to scramble to review its security.

## The Bigger Idea

One of the most important lessons in all of security has nothing to do with hacking: **data you think is harmless can become dangerous when you aggregate it**. One person's jog is nothing. Millions of jogs, combined and mapped, is military intelligence. The sensitive information wasn't in any individual data point - it *emerged* from the pile.

That's the difference between data and metadata. The content of a run ("someone exercised") seems trivial. The metadata around it - where, when, how often, in what pattern - can be the whole story. Attackers and analysts love metadata precisely because people guard their "content" and give their location away for free. Your phone is doing some version of this right now, and most of the settings that control it default to *on*. For example - do your photos store the location and time they were taken?

## Why This Is Tricky

The seemingly obvious response - "turn off location" - has real costs. Location makes maps, ride-shares, fitness goals, and "find my phone" work. Strava's users *wanted* to share their routes; that was the point. So the question isn't whether location data is useful. It's who should bear the risk of the surprising things it reveals when combined - the individual who clicked "allow," or the company that designed the default.

## Step 1 - Read

The first two tell the Strava story and the response; the third shows how investigators still use this kind of open location data, so you see why it's powerful.

- **The discovery (CNN)** - the U.S. military reviews security after a fitness app reveals sensitive info. https://www.cnn.com/2018/01/28/politics/strava-military-bases-location
- **The response (Engadget)** - after exposing secret bases, Strava restricts data visibility. https://www.engadget.com/2018-03-13-after-exposing-secret-military-bases-strava-restricts-data-visi.html
- **Why it matters (GIJN)** - how investigators use the Strava app to find things. https://gijn.org/stories/investigations-using-strava-fitness-app/

## Step 2 - Research on Your Own

Find **at least four more** reputable sources you dig up yourself - news reporting, another location-data exposure (search "Life360" or "geofence warrant"), or a security guide to app location permissions. Random social-media posts don't count. You'll cite these in your paper and lean on them in the debate.

## Step 3 - Written Response

Turn in a typed paper. Answer in complete sentences. Point values are shown; total is **25 points**.

### Comprehension

1. What exactly did the Strava heatmap reveal, and how - given that nothing was "hacked"? (1 pts)
2. Explain the difference between the *content* of your location data and its *metadata*, with an example. (1 pts)

### Analysis

1. Who benefits from location-sharing features, and who bears the risk? Name at least two groups on each side and explain each. (2 pts)
2. "One jog is nothing; a million jogs is intelligence." Explain, in your own words, how aggregating harmless-looking data can produce sensitive information that isn't in any single piece. (3 pts)
3. I play a lot of Pokémon Go - it's even led me to Lord of the Rings filming spots in New Zealand that aren't marked on Google Maps. But here's the flip side: every player walking around catching Pokémon is also feeding a constant stream of location data back to the company behind the game. Using the aggregation idea from the question above, explain what that company could learn from millions of players' movements - and whether the fun is worth what players hand over. (3 pts)
4. Whose responsibility was the base exposure - the individual soldiers who left location on, or Strava for defaulting it on and publishing it? Take a position and support it with evidence. (5 pts)

### Position

Take a clear position on the resolution below and argue it - this is the required part.

1. Where do you stand on the resolution? Argue your side using evidence from at least two of the sources you found, then fairly state the single strongest argument against your view and respond to it. (10 pts)

### (OPTIONAL) Prepare Both Sides

Your teacher may ask you to be ready to argue *either* side. If so, also prepare a short case for each:

1. The strongest case **FOR** the resolution, backed by evidence you found yourself.
2. The strongest case **AGAINST** the resolution, backed by evidence you found yourself.

## Step 4 - (OPTIONAL) Class Debate

**Resolved:** *"Apps should be required to turn location-sharing OFF by default."*

If your teacher runs the debate, you'll defend a position on this resolution, and you may be **assigned a side at random** - which is why the optional prep above asks you to be ready for both. You won't have your paper or notes with you, so know your evidence well enough to argue from memory.

**Two rules make the debate work:**

**1. Evidence only.** Every claim points to a specific source for evidence, not a feeling.

**2. Steelman first.** Before you rebut the other side, restate their strongest argument fairly enough that they'd nod along. Then tell your tale.

## One More Thing

Most people picture a "hack" as someone breaking in. This one was just people sharing freely, plus someone paying attention. That's the kind of security risk most people never think about - and the one most likely to matter in your life: not a villain at a keyboard, but the quiet, surprising power of data you gave away without thinking.

READING & WRITING ASSIGNMENT

# An Army of Baby Monitors

*The Mirai Botnet and Insecure Smart Devices*

## The Story That Started This

On October 21, 2016, big chunks of the internet simply stopped working. Twitter, Netflix, Reddit, Spotify, GitHub - all unreachable for hours. The target wasn't any of those sites. It was **Dyn**, a company that runs part of the internet's phone book (DNS). And the weapon was one of the strangest armies ever assembled: hundreds of thousands of **home security cameras, baby monitors, and routers**, all taken over and pointed at Dyn at once, peaking at over a terabit of traffic per second.

The malware was called **Mirai**. It wasn't sophisticated - you could probably recreate it fairly easily. Mirai spread by trying a list of about 60 common factory-default passwords - "admin/admin," "root/12345" - against internet-connected devices. Millions of gadgets had shipped with those passwords and nobody ever changed them. Even stranger, Mirai was written by a few college-age guys who mainly wanted an edge in *Minecraft*. They released the source code publicly, and copycats have been building on it ever since.

## The Bigger Idea

A botnet is a network of devices infected with malware and controlled remotely by an attacker. Individually, a hacked baby monitor is harmless. Networked together by the tens of thousands, those devices become a cannon capable of knocking real services offline in a distributed denial-of-service (DDoS) attack.

The key lesson is about **defaults and externalities**. The camera worked perfectly for its owner, so nobody noticed or cared that it was insecure - the harm landed on *other people* (Dyn, and everyone who couldn't reach Twitter). The manufacturer saved a few cents by shipping a pre-configured default password. That tiny, invisible decision, multiplied across millions of devices, became an internet-scale weapon. Security you can't see is exactly the security people skip.

## Why This Is Tricky

Whose fault is a Mirai device? The owner never changed the password - but most owners don't know a baby monitor *has* a password, or what a botnet is. The manufacturer shipped it insecure - but secure practices cost money and likely support headaches, and consumers reward whoever's cheapest and easiest to use. Regulation could force better security - but it could also raise prices and slow down a huge, useful industry. There's no simple answer.

## Step 1 - Read

The first explains Mirai in depth; the second draws out the IoT-security lessons; the third is the government's alert from the time.

- **The story (CSO Online)** - how teen scammers and CCTV cameras almost brought down the internet.
  https://www.csoonline.com/article/564711/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html

- **The lessons (Stanford)** - the 2016 Dyn attack and what it taught us about IoT security.
  https://mse238blog.stanford.edu/2018/07/clairemw/the-2016-dyn-attack-and-its-lessons-for-iot-security/

- **The official alert (CISA)** - the heightened DDoS threat posed by Mirai and other botnets.
  https://www.cisa.gov/news-events/alerts/2016/10/14/heightened-ddos-threat-posed-mirai-and-other-botnets

## Step 2 - Research on Your Own

Find **at least four more** reputable sources you dig up yourself - technical write-ups of Mirai, a more recent IoT botnet, or a law like California's IoT default-password ban (SB-327). Random social-media posts don't count. You'll cite these in your paper and lean on them in the debate.

## Step 3 - Written Response

Turn in a typed paper. Answer in complete sentences. Point values are shown; total is **25 points**.

### Comprehension

1. How did Mirai actually take over devices, and what did it then use them to do? (2 pts)
2. What is a botnet, and why was a DNS provider like Dyn such a damaging target? (2 pts)

### Analysis

1. Who benefits from cheap, convenient smart devices, and who bears the risk when they're insecure? Name at least two groups on each side. (3 pts)
2. This is a classic example of "externality": the insecure device works fine for its owner while harming others. Explain that idea using Mirai, and why it makes IoT security so hard to fix through consumer choice alone. (3 pts)
3. Mirai spread through default passwords - an issue that would take one-line to fix, technically. So why does this keep happening? Argue where the responsibility should sit, and provide support with evidence. (5 pts)

### Position

Take a clear position on the resolution below and argue it - this is the required part.

1. Where do you stand on the resolution? Argue your side using evidence from at least two of the sources you found, then fairly state the single strongest argument against your view and respond to it. (10 pts)

### (OPTIONAL) **Prepare Both Sides**

Your teacher may ask you to be ready to argue *either* side. If so, also prepare a short case for each:

1. The strongest case **FOR** the resolution, backed by evidence you found yourself.
2. The strongest case **AGAINST** the resolution, backed by evidence you found yourself.

## **Step 4** - (OPTIONAL) **Class Debate**

**Resolved:** *"Manufacturers should be legally responsible for the security of the smart devices they sell."*

If your teacher runs the debate, you'll defend a position on this resolution, and you may be **assigned a side at random** - which is why the optional prep above asks you to be ready for both. You won't have your paper or notes with you, so know your evidence well enough to argue from memory.

**Two rules make the debate work:**

**1. Evidence only.** Every claim points to a specific source for evidence, not a feeling.

**2. Steelman first.** Before you rebut the other side, restate their strongest argument fairly enough that they'd nod along. Then tell your tale.

## One More Thing

Someday you may ship code that runs on a device somebody buys and forgets about. Mirai is a reminder that "it works" and "it's secure" are not the same thing - and that the gap between them can, quite literally, wreck the internet. Please don't, Ralph.

s

READING & WRITING ASSIGNMENT

# The Weapon That Got Away

*Vulnerability Disclosure, EternalBlue, and WannaCry*

## The Story That Started This

The U.S. National Security Agency (NSA) found a flaw in the Windows Operating System (OS) - a serious one, in how Windows shared files across a network. Instead of quietly telling Microsoft so it could be fixed, the NSA kept the flaw secret and built a hacking tool on top of it, codenamed **EternalBlue**. They held onto it as a weapon for more than five years.

Then, in 2017, a group called the Shadow Brokers stole the NSA's toolkit and dumped EternalBlue on the open internet. Microsoft rushed out a patch, but millions of machines did not install it. A month later, ransomware called **WannaCry** - built on the NSA's leaked exploit - tore through more than 230,000 computers in 150 countries, freezing hospitals, factories, and the UK's National Health Service, where surgeries were cancelled and ambulances diverted. A 22-year-old researcher named **Marcus Hutchins** accidentally found a "kill switch" in the code and stopped it almost by luck. The government's secret weapon had become everyone's disaster.

## The Bigger Idea

Every time a government (or a researcher, or a company) discovers a software vulnerability, it faces a genuine dilemma called the **vulnerabilities equities problem**: *disclose* the flaw so it can be patched and everyone gets safer, or *keep* it secret to use for spying and offense. You can't do both - the same hole that lets you break into an adversary's system is the hole that leaves your own hospitals exposed. A vulnerability is not "ours" or "theirs." It's just a hole in software everyone uses.

EternalBlue is the cautionary tale for the "keep it" side: a stockpiled weapon leaked and came home. It even pushed Microsoft to call for a "Digital Geneva Convention" banning governments from hoarding vulnerabilities. But the "keep it" side has a real argument too - intelligence and national defense sometimes depend on exactly these tools.

## Why This Is Tricky

If the NSA discloses every flaw it finds, it gives up real intelligence capabilities that other nations may not give up as freely. This could give other nations a tactical advantage. If the NSA hoards flaws... well, EternalBlue shows what happens when the vault gets robbed. And "the government" isn't one actor - the agency that wants to attack and the agency that wants to defend citizens are sometimes the same government pulling in opposite directions. There's no clean answer, which is why professionals still argue about it.

## Step 1 - Read

The first two explain EternalBlue and WannaCry; the third is the human story of the researcher who stopped it - and later got arrested, which complicates everything nicely.

- **The exploit (Avast)** - what EternalBlue is and why the leaked NSA tool still matters.
  https://www.avast.com/c-eternalblue
- **The attack (Cloudflare)** - what the WannaCry ransomware attack was and how it spread.
  https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/
- **The human (WIRED)** - the confessions of Marcus Hutchins, the hacker who saved the internet.
  https://www.wired.com/story/confessions-marcus-hutchins-hacker-who-saved-the-internet/

## Step 2 - Research on Your Own

Find **at least four more** reputable sources you dig up yourself - reporting on the Shadow Brokers, the U.S. "Vulnerabilities Equities Process," Stuxnet or SolarWinds, or Microsoft's Digital Geneva Convention proposal. Random social-media posts don't count. You'll cite these in your paper and lean on them in the debate.

## Step 3 - Written Response

Turn in a typed paper. Answer in complete sentences. Point values are shown; total is **25 points**.

### Comprehension

1. Trace the chain of events from the NSA's discovery of the flaw to the WannaCry outbreak. (2 pts)
2. In your own words, what is the "vulnerabilities equities" dilemma? (2 pts)

### Analysis

1. Who benefits when a government stockpiles a vulnerability, and who is put at risk? Name at least two groups on each side. (3 pts)
2. "A vulnerability is not ours or theirs - it's a hole in software everyone uses." Use EternalBlue to explain why that makes stockpiling so dangerous. (3 pts)
3. Does the intelligence value of keeping a flaw secret ever outweigh the public risk? Take a position and support it with evidence from a real case. (5 pts)

### Position

Take a clear position on the resolution below and argue it - this is the required part.

1. Where do you stand on the resolution? Argue your side using evidence from at least two of the sources you found, then fairly state the single strongest argument against your view and respond to it. (10 pts)

### (OPTIONAL) **Prepare Both Sides**

Your teacher may ask you to be ready to argue *either* side. If so, also prepare a short case for each:

1. The strongest case **FOR** the resolution, backed by evidence you found yourself.
2. The strongest case **AGAINST** the resolution, backed by evidence you found yourself.

## Step 4 - (OPTIONAL) Class Debate

**Resolved:** *"Governments should be required to disclose the software vulnerabilities they discover, rather than stockpile them as cyber-weapons."*

If your teacher runs the debate, you'll defend a position on this resolution, and you may be **assigned a side at random** - which is why the optional prep above asks you to be ready for both. You won't have your paper or notes with you, so know your evidence well enough to argue from memory.

**Two rules make the debate work:**

**1. Evidence only.** Every claim points to a specific source for evidence, not a feeling.

**2. Steelman first.** Before you rebut the other side, restate their strongest argument fairly enough that they'd nod along. Then tell your tale.

## One More Thing

This is the kind of decision real security professionals and governments wrestle with - no clean answer, enormous stakes. If you go into this field, you may someday be the person who finds the flaw and has to decide what to do with it. And when there's no rulebook to tell you the right move, the only thing left to rely on is your own judgment - so start practicing it now.

READING & WRITING ASSIGNMENT

# Pay or Bleed

*Ransomware and the Impossible Choice*

## The Story That Started This

You already lived through one of these.

In May 2026, during finals for a lot of schools, the learning platform **Canvas** was hit. A group called ShinyHunters breached Instructure, the company behind Canvas, and stole data tied to as many as **275 million people across roughly 9,000 schools** - usernames, emails, course info, messages. Parts of Canvas went dark right when students needed them most. One day before the attackers' deadline to leak everything, Instructure **paid the ransom**. Your coursework, your messages, your name were part of what was on the line.

Now scale that up until lives are at stake. In February 2024, ransomware hit **Change Healthcare**, which processes about half of all U.S. medical claims. Pharmacies couldn't fill prescriptions, hospitals couldn't get paid, and roughly **190 million people** had data exposed. Change's parent company paid about **$22 million** - and then a *second* criminal group popped up claiming to hold the same data and demanded to be paid again. Total damage: over $1.5 billion. Same impossible question, at both scales: when criminals hold your data hostage, do you pay?

## The Bigger Idea

Ransomware is malware that encrypts a victim's data (or threatens to leak it) and demands payment for the key or for silence. What makes it uniquely nasty is that it turns a technical break-in into an **economic and ethical decision**. The encryption is just the setup to the real weapon - the choice it forces you to make.

And it's genuinely a dilemma. Paying can be the fastest way to restore care or protect people's data - so a hospital administrator watching patients suffer has a reasonable human reason to pay. But every payment funds the next attack, marks you as someone who pays, and - as Change Healthcare learned - buys you nothing enforceable, since criminals can simply come back for more. Refusing is principled and starves the business model, but the cost of refusing can be measured in cancelled surgeries and leaked records. There's no option where nobody gets hurt.

## Why This Is Tricky

You've heard a version of this before: the United States famously says it doesn't pay ransoms or negotiate with terrorists - on exactly this logic, that every payment funds the next attack and marks you as someone who pays. A law barring ransomware payments would work the same way, making targets less profitable over time and maybe shrinking the whole industry. But the hard line runs into a hard reality. Barring payment punishes the victim at the worst possible moment and could push payments underground. "Never negotiate" is easy to say from a distance and agonizing when the hostage is a hospital - or your own school. And notice: even that famous no-ransom stance has bent in practice when real lives were on the line. That gap between the principle (theory) and the moment (reality) is exactly what you'll face in the assignment.

## Step 1 - Read

The first covers the Canvas breach that hit students directly; the second and third cover Change Healthcare and the payment dilemma.

- **The one you lived (National Cybersecurity Alliance)** - the Canvas data breach and what it means for students.
  https://www.staysafeonline.org/articles/canvas-data-breach

- **The high-stakes case (Wikipedia)** - the 2024 Change Healthcare ransomware attack.
  https://en.wikipedia.org/wiki/2024_Change_Healthcare_ransomware_attack

- **The bigger trend (IBM)** - ransomware and healthcare-industry attack trends.
  https://www.ibm.com/think/insights/healthcare-industry-attack-trends-2024

## Step 2 - Research on Your Own

Find **at least four more** reputable sources you dig up yourself - reporting on a specific ransomware attack, FBI or CISA guidance on whether to pay, or a proposed ransom-payment ban. Random social-media posts don't count. You'll cite these in your paper and lean on them in the debate.

## Step 3 - Written Response

Turn in a typed paper. Answer in complete sentences. Point values are shown; total is **25 points**.

### Comprehension

1. What is ransomware, and what makes it different from an attack that simply steals data? (1 pts)
2. In the Change Healthcare case, what happened *after* the company paid - and what does that reveal about paying? (1 pts)

### Analysis

1. Who is helped and who is harmed when a victim pays a ransom? Name at least two groups on each side and explain each. (2 pts)
2. How can individuals and companies protect themselves from ransomware? Describe at least 2 ways and any associated costs. (3 pts)
3. Explain why ransomware turns a technical problem into an economic one - and why "just restore from backups" isn't always a real option. (3 pts)
4. **The one that hit you:** Instructure paid to keep your Canvas data from leaking. Was that the right call? Explain what paying accomplished for students, what it may have encouraged, and whether you'd have decided the same. Use evidence. (5 pts)

### Position

Take a clear position on the resolution below and argue it - this is the required part.

1. Where do you stand on the resolution? Argue your side using evidence from at least two of the sources you found, then fairly state the single strongest argument against your view and respond to it. (10 pts)

### (OPTIONAL) Prepare Both Sides

Your teacher may ask you to be ready to argue *either* side. If so, also prepare a short case for each:

1. The strongest case **FOR** the resolution, backed by evidence you found yourself.
2. The strongest case **AGAINST** the resolution, backed by evidence you found yourself.

## Step 4 - (OPTIONAL) Class Debate

**Resolved:** *"Organizations should be legally barred from paying ransomware demands."*

If your teacher runs the debate, you'll defend a position on this resolution, and you may be **assigned a side at random** - which is why the optional prep above asks you to be ready for both. You won't have your paper or notes with you, so know your evidence well enough to argue from memory.

**Two rules make the debate work:**

**1. Evidence only.** Every claim points to a specific source for evidence, not a feeling.

**2. Steelman first.** Before you rebut the other side, restate their strongest argument fairly enough that they'd nod along. Then tell your tale.

## One More Thing

You were a single data point in one of the biggest school breaches in history, and Instructure paid to "protect you". How does that make you feel? Sit with the uncomfortable questions that come with that, and remember every solution has a cost in real life.