Name: Mia Ash (possibly)
Skills: Hacking
Most noteable for: Being Iranian state-sponsored hackers that targeted individuals with senior roles, and attempted to assault them with malicious macros.

REX FEATURES, ALLSTAR, NICOLA DOVE/DANJAQ, LLC AND MGM, DREAMSTIME

PROFILE UPDATE FOR THE MODERN SPY

What is the profile of the real-world secret service agent? What do they look like? What skills does the person have? *E&T* tried to find clues, but the answer may surprise you – and it's far from the ageing 'technotard' that is Daniel Craig's James Bond.

By **Ben Heubl**

WHEN A COY Facebook profile with the name of Mia Ash began to contact men in senior positions – many of them with access to computer networks – it did not arouse any suspicion.

When it turned out to be a trap by Iranian state-sponsored hackers, it may have dawned on some that behind Mia Ash there was something more than an enchanting, young, female photographer.

The cover was blown for the espionage campaign when a security analyst at Secureworks, a US cyber-security company, spotted an employee's conversation with Mia Ash. Conversations began on LinkedIn, then moved to Facebook. Eventually, the employee received an email with a Microsoft Excel attachment for a photography survey. It contained an assault with a malicious macro meant to infect the receiver's computer.

To Edward Lucas, a British journalist, this example of modern-day espionage stands out. It exemplifies how the world has changed in the wake of technology. "Victim A did not need to be particularly interesting as an intelligence source. He did not need to know any secrets. The only thing that mattered was that he had access to his company computer network," Lucas says in his book 'Spycraft Rebooted: How Technology is Changing Espionage'.

Mia Ash not only teaches us about modern spies' latest schemes, it is also a lesson in how much effort goes into it creating the charade. Next to the Facebook and Linkedin profile, there was also a blog set up which was active for almost a year before the whole operation blew up. It had garnered over 500 LinkedIn connections, some being legitimate photographers. The social-media spy is now an established strategy, experts say, and the trend towards these profiles is only growing, according to a researcher at Secureworks.

Online social-media spies are not the only contemporary secret agents who paint the town red. There are the real-life ones behind the curtain, many of them now spending most of their time at computers and much less time locating potential dead-drops.

Behind the smoke and mirrors game, one thing seems certain: the description of modern intelligence agents does not fit fictional movie heroes like James Bond. Mentioning Bond to ex-intelligence officers merely provokes a chuckle.

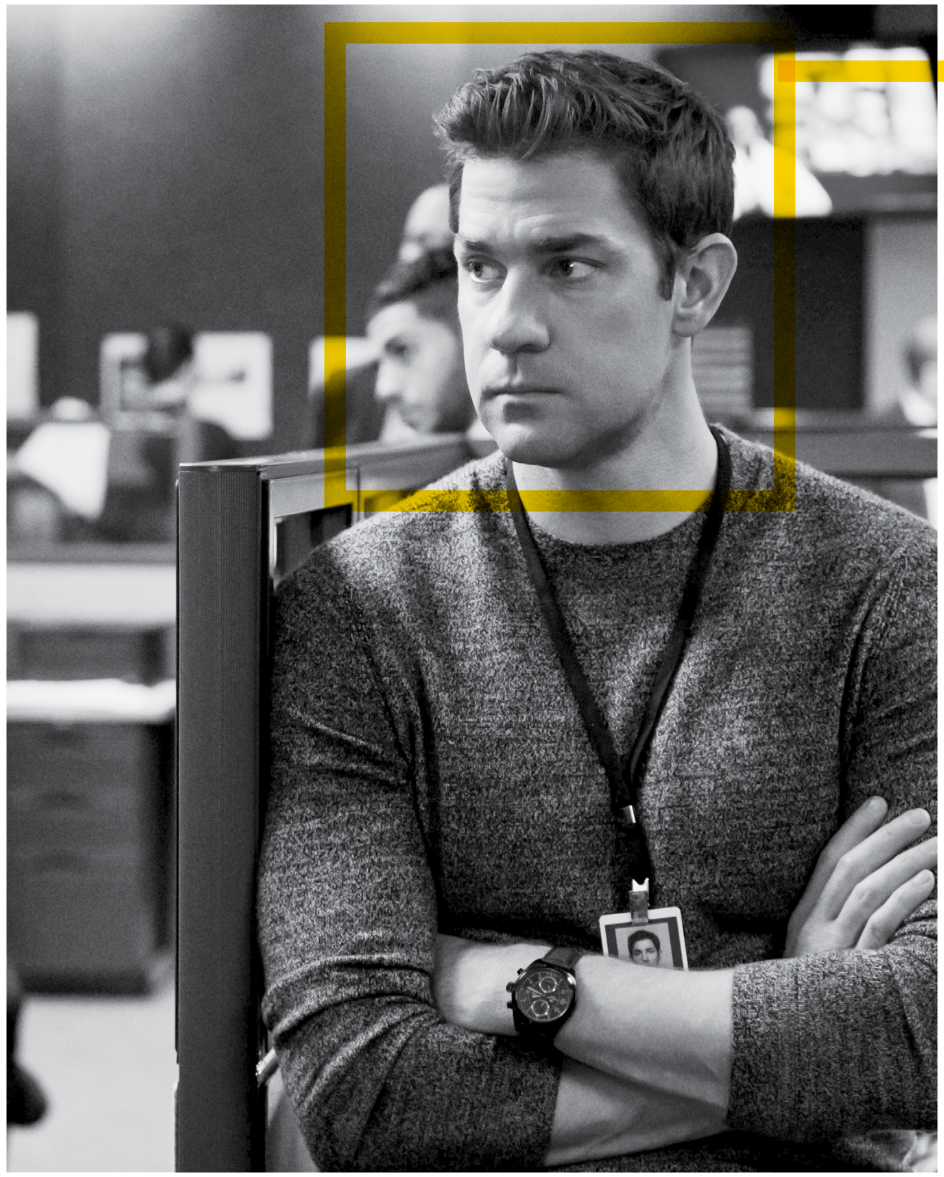
The reality of today's tech-savvy spies is much dorkier: "From my experience, they tend to be nerdy, definitely not as cool as in Hollywood. Sometimes they're just weird," says Charity Wright, a former senior intelligence officer at the US National Intelligence Agency (NSA) who is now a cyber-threat intelligence analyst.

Wright's comments fit the profile depicted by other sources from inside intelligence agencies too. For example, the ongoing trial for treason against disgruntled CIA employee Joshua Schulte shows the internal working climate among developers with security clearance. Schulte is accused of stealing and leaking classified information to Wikileaks. He and his colleagues do not fit the typical Hollywood image because they "sent each other prank emails", "taunted each other about their physical appearances" and were "shooting at each other with Nerf guns", according to a *New York Times* report. What was Schulte's motive? The computer engineer grew frustrated because his manager did not take his workplace complaints seriously.

Disgruntled staff causing trouble is a problem the CIA is all too familiar with. Edward Lee Howard, an ex-CIA trainee fired in 1983 because he failed a routine polygraph test – it indicated he lied about past drug use – is believed to be behind the exposure of one of America's most valuable Soviet intelligence sources. Adolf Tolkachev was a Soviet electronics engineer and a chief designer at Phazotron, the Soviet radar design bureau. He provided valuable information to the US agency until his arrest in 1985. He was executed in 1986. Tolkachev became the central hero of the non-fiction book by David E Hoffman, 'The Billion Dollar Spy: A True Story of Cold War Espionage and Betrayal'.

Leaking intelligence

Tolkachev is a textbook example of the presence of tech-savvy staff and agents in the increasingly technology-driven world of espionage. It was partly his technical knowledge and engineering degree that made his contribution to the CIA so invaluable. Tolkachev leaked intelligence on Soviet >



Name: Dr Jack Ryan
Skills: Financial analyst and later head of the CIA's Terror, Finance and Arms Division under the Counterterrorism Center.
Most noteable for: Being most like the spy of today.

< aircraft, radar and weapons guidance systems via a James Bond-esque miniature Pentax camera, or via memorisation and jotting it down. Fast-forward four decades and conditions have changed. Technology has advanced, but agencies' questions about adversaries have not. Arguably, there is an even larger need to reverse-engineer opponents' techniques.

How did the agent's profile evolve over time? Wright says modern NSA intelligence officers still tend to be predominantly white, and the odds of meeting a female officer are low. Gender diversity is a problem even now; the number of female officers in the intelligence section is only slightly better than for the US military, with Wright estimating the sector to be around 25 per cent female.

An appetite to hire tech-savvy recruits changes secret service agencies. Sometimes, recruits bring tech skills to the job, while occasionally they are trained in-house, Wright says. This appetite also changed how new recruits are scouted. "The days when intelligence agencies recruited through the common rooms of Oxbridge are thankfully behind us," says Malcolm Taylor, director of cyber security for ITC Secure. "You need people who understand technology." Taylor is an ex-senior intelligence officer who served overseas in Afghanistan, Iraq and Pakistan.

The British secret intelligence service (SIS) is not hiding its aspirations to hire tech and engineering talent. For years, its recruitment page fished for positions like 'software engineering specialists' because "technology is behind everything we do", a recent advertisement claims. SIS's selling point is that it "makes working in our Science and Technology teams varied, challenging and always exciting".

Open-source intelligence (OSINT) to be used for counter-intelligence is now centre of the debate among Western secret service agencies. Cases like Mia Ash contributed to this. Being good at handling open source intelligence "and, put crudely, being good at Googling, is a real skill in the intelligence world," Lucas says. Being an OSINT expert is now a whole career path.

The value of OSINT came as the internet grew from being a minor part of the intelligence world to a much bigger one. One paradox lies in conflict of the raw data everyone can access online, versus the intelligence it provides, which can be classified as secret and valuable. Lucas explains: "Although an OSINT assessment can be entirely based on unclassified sources, the resulting product can be quite highly classified. It is because you can work out, from the way it is put together, what other things the government in question knows or what it thinks is interesting."

The power of OSINT

So what is OSINT? Open-source intelligence-gathering techniques can be as mundane as searching through online databases, for instance searching the online yellow pages – a service like 192.com can spit out details on someone's home address and who has lived at that address in the past.

OSINT is a way of categorising intelligence information; it is all about connecting the dots. It can come from a satellite, from a human source, or even a cryptographic breakthrough. US and UK intelligence services are adamant that they hire recruits who have such skills, with a CIA job advert looking for "Open Source Collection Officers" and the UK's MI5 and MI6 advertising for "cyber apprenticeships, with a special focus on OSINT".

In the last few years, agencies took note of the power of open-source intelligence. "It was big when I was there, but since then it must have only grown in importance [for the British foreign intelligence service]," Taylor says. It would also be no surprise if secret service agencies took interest in databases such as the IET's 'Inspec' platform, a large scientific and technical database.

Today's spies take an interest in open-source 'jigsaw puzzles' because of their cost effectiveness, while Western spies must jump through several hoops to get access to more advanced espionage techniques that require approval, such as phone tracking. In an age of fear of mass surveillance among the public, Western secret-service agencies come under tremendous pressure to comply with the law. On the upside, open-source intelligence can be gathered quite legally. This does not mean that privacy experts wholeheartedly approve.

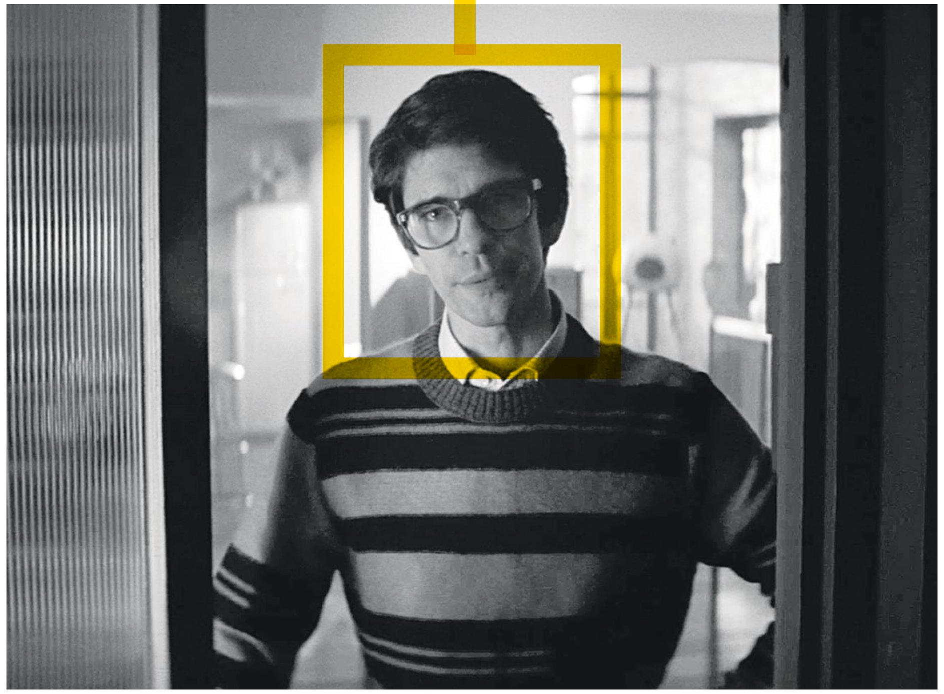
Allison Wikoff, a senior security researcher at Secureworks, says open-source intelligence could easily have spotted the counterfeit nature of the account of Mia Ash: "The funny thing about all of these personas is that if you look at them for who they claim they are, it doesn't make any sense. Ash was a young woman based in London who was running her own photography business. But if you looked at any of her pages and blog, what sort of photographer running their own business has no website, and no contact information? Some images still had a watermark on them."

At its most basic level, prudent Googling techniques, so-called 'Google dorking', can bring benefits to agents. More advanced OSINT techniques can run programs that gather data from hundreds of sites in minutes.

It transpires that the real-life modern agent may have a lot more in common with a cautious data privacy advocate than with James Bond. Privacy advocates like Michael Bazzell, author of OSINT training literature, writes and talks in his podcast about ways to dodge data tracking by commercial and government agencies. He stresses that his books are not a how-to guide for criminals to steal identities; no methods described in the latest 550+ page book are illegal.

However, because modern espionage is all about finding solutions to keep identities undetected, the same methods may apply to intelligence agents and officers. "The most prized ability in real spy craft is the ability to blend into your surroundings to the point that nobody really notices you," Lucas writes in his book.

Name: Q
Skills: Hacking, making gadgets, MI6's resident geek. Head of Q Branch, a fictional division of the British Secret Service.
Most noteable for: Creating simple, yet effective spy gadgets for 007. "Can do more damage on his laptop in his pyjamas than Bond can do in a year in the field."



Name: M
Skills: The head of MI6 and Bond's superior.
Most noteable for: In 'Golden Eye', she calls Bond a "sexist, misogynist dinosaur, a relic of the Cold War". Known as the 'Evil Queen of Numbers', she relies on stats and analysis rather than impulse and initiative.

> 'The Snowden files contain evidence that US and British intelligence agencies made good use of virtual gaming communities. Since 2008, they used them to spy and for informant recruitment purposes.'

Undeniably, big tech's social networks added a wealth of new data and possibilities to the modern open-source intelligence work. Bazzell's latest book dedicates more than 20 pages-worth of techniques solely to Facebook's platform, while other social media receive similar attention.

Facebook used to be even better for OSINT as it linked a phone number to an account – phone numbers can be an important connector between accounts and identities – until the company shut it down because it understood that criminals can scrape users' public profiles for malicious purposes.

Phoneinfoga, another open-source option, can tell whether a phone number is disposable or legitimate. A throwaway number may raise questions to agents about a person's or an account's identity.

Explicit concerns

As potential targets leave a trail of their potentially sensitive personal information along the way, open-source online forums and social networks like Twitter can be a common playground for espionage. They can reveal hobbies, connections and weaknesses agents can later exploit.

More than four decades ago, Oleg Gordievsky, a KGB agent, was only picked up as a double-agent candidate by the British when he was overheard expressing dissatisfaction with the Soviet system. Today, someone like Gordievsky might leave clues across a plethora of online profiles and blog posts, which the OSINT-trained agents can pick up on.

If investigators paid close attention to open-source forum entries made by Edward Snowden to the Ars Technica forum under his pseudonym 'TheTrueHOOHA', they might have picked up on his distaste for Barack Obama's appointment of CIA director Leon Panetta, or his explicit concerns for pervasive government surveillance made in February 2010.

LinkedIn is also a hotspot for agents targeting Western users. Wikoff says it is popular among Iranian agents to pose as recruiters from defence contracting companies or agencies, to befriend profiles with IT positions and anyone with access to computer networks. She adds: "[Linkedin] is a professional network and people don't think about it being used for nefarious purposes."

Last year, a *New York Time*s report explained how Chinese agents went after foreign citizens via profiles on LinkedIn, with former government officials among those targeted. Unfortunately, we may not have seen the end of it as the strategy seems successful. One former employee of the CIA and Defense Intelligence Agency lured into spying for China in this way was sentenced to 20 years in prison.

Online multiplayer gaming chat rooms also appear to be popular hunting grounds among modern spies. The Snowden files contain evidence that US and British intelligence agencies made good use of virtual-gaming communities. Since 2008, they used them to spy and for informant recruitment purposes.

Amazon's user data also adds its share. Via its native 'wish list' search option, any name or email address can reveal a target's product wish list, baby or wedding registry. If the agent needs to check a username across other social media networks, such as from an account set up by the Islamic State (ISIS), knowem.com analyses more than 500 other websites. If an agent just has an online image to go on, OSINT's TinEye image recognition can compare it with 39.7 billion others on the web. Should an agent need to exploit system vulnerabilities, the open-source system vulnerability search engine Shodan can be of service. The list of OSINT tools goes on and is constantly updating. Tools disappear and websites stop offering services, but new ones pop up out of the blue. >

Name: Bond – James Bond
Skills: Strategist, detective, multilingualist, persuasion/seduction, physical fitness, combat, assassin, marksman.
Most noteable for: Not having time to die.

< Taylor mentions the 46,000 Twitter accounts ISIS used to operate. "The vast majority of it is nonsense, then a lot of it is propaganda. But there is some valuable information. A photograph, the background in a photo, an account or user name... a skilled person can build a whole picture of an individual," he says.

Naturally, OSINT techniques have limits. Secret intelligence agencies know this. "To say whether someone has a mobile phone, it's not OSINT because to do that you must have some kind of clandestine illegal technical means to find it out," Lucas explains. "Once I begin to want to know where you had breakfast this morning, I have to hack into your mobile phone or have access to your mobile phone provider and I need to have access to CCTV cameras on the streets."

Agents from totalitarian regimes like in China and Russia are said to have more wiggle room to apply these advanced non-open-source techniques, with little scrutiny by the public and state. Taylor describes the difference between Russian and Chinese secret intelligence staff and their Western counterparts. "The Russians are very blunt, and they care much less about getting caught, [they are] less nuanced, and they achieve their aims less often.

"Brexit and Donald Trump are massive exceptions," he adds. "The Chinese have money, people and military capabilities. They are much more subtle than the Russians."

'The sector has an image problem. To overcome this, increased transparency may be necessary, but this goes against the DNA of a 'secret' service.'

Although Western agents from democracies may have more leeway in applying non-open-source espionage techniques, they have one essential advantage in his view: they might sleep much better at night. Taylor thinks Western agents "do[ing] things rigorously and in the right way" pays off: "You are usually more successful."

The modern agent

The agent Taylor describes is anything but the rule-breaking action hero with a Bond-like ego. Rule-abiding intelligence agencies in the West have an edge over others: "Look where the best intelligence services are in the world – the UK, the US, France, Germany, Israel... but it might be slightly different. They are Western democracies with lots of regulation around."

Apart from technical and operational obstacles, the biggest challenge faced by Western modern secret intelligence agencies is image and trust. To gain confidence from the public and politicians is not a cakewalk (Edward Snowden for example), and fictional secret agents like Bond don't help because of their misrepresentation of reality.

Intelligence analyst Wright and ITC Secure's Taylor admit the sector has an image problem. To overcome this, increased transparency may be necessary, but this goes against the DNA of a 'secret' service. Additionally, they are losing agents and intelligence officers to the private market. It is no coincidence that Wright and Taylor ended up in the cyber-security sector after leaving their posts.

Wright says: "The private sector pays way better than the government sector. I think the NSA realises they're bleeding out people to the private sector so they're trying to work on that and create better compensation packages to keep people.

"It's not easy to be up against these cyber-security companies making good money," she adds. Many of her colleagues and contacts in other cyber-security firms used to do government intelligence work, while her starting salary at her job in cyber security was about $30,000 a year more than she expected.

As the 25th instalment of the James Bond franchise drops soon in cinemas – with Daniel Craig in his final outing as the British spy – the question is: do the screenwriters give Bond the benefit of retiring into a cushy role in the private sector?

I think we all know the answer to that... there is no time to die. *