December 2020

USS Pueblo, John Walker and KGB

Robert Derenčin

Capture of USS Pueblo in January 1968

In January 1968 the US Navy ship Pueblo was on an electronic reconnaissance mission off the east coast of North Korea. Arriving on January 16 south of Vladivostok (and the border of the Soviet Union and North Korea) Pueblo headed south, along the North Korean coast, remaining permanently in international waters, staying for some time in front of the ports of Ch'ongjin, Kimch'aek, Mayang-do Island (submarine base of the North Korean Navy) and finally Wonsan.

On January 23 (noon) in the front of Wonsan North Korean Navy ships (one submarine chaser and 4 torpedo boats) surrounded Pueblo demanding that Pueblo follow them towards Wonsan. Two North Korean MiG-17s flew over Pueblo. Commander of Pueblo Commander Bucher, manoeuvred to take Pueblo further out to sea, but after artillery and machine gun fire was opened on Pueblo (during which one Puebla crew member was mortally wounded) Bucher was eventually forced to surrender the ship (Newton 1992). For the 82 surviving Pueblo crew members, this was the beginning of 11-months long captivity (USS Pueblo).

There are theories how the North Korean knew that Pueblo was reconnaissance ship, were the North Koreans knew about the arriving of Pueblo etc. The answer is very simple. Immediately after Pueblo came near North Korean coast she was detected by North Koreans radars and then her moving was followed. By the way Pueblo navigated it was clear she was reconnaissance ship.

The North Koreans attacked Pueblo in the front of Wonsan because it was the most suitable place for the attack. That part of the coast is retracted inland, if sailing in front of Wonsan the ship is surrounded on three sides by North Korean territorial waters. It means that the only way Pueblo could manoeuvre to try to get the open sea was eastward, and even the Americans had sent their airplanes to help, they wouldn’t be able to operate without entering North Korean airspace.

Compromise of classified information resulting from the capture of USS Pueblo

At the time of the capture of Pueblo, the US Navy used all possible means of radio communication, radio-telephony, radio-telegraphy, and radio-teleprinter communication, on all radio-frequency bands. At the strategic level, the most important type of radio communication was HF (High Frequency, 3 to 30 MHz) radio-teleprinter communication. There were few ciphering systems which protected secrecy of the messages, and on Pueblo the North Koreans found the following ciphering machines: KL-47 (1 pc.), KW-7 (2 pcs.), KWR-37 (3 pcs.) and KG-14 (4 pcs.), also spare parts, keys and instructions for use and maintenance of the mentioned machines (Cryptographic damage, Report).

The KW-7, KWR-37 and KG-14 machines were connected between radios and teleprinters and worked automatically, which means that they were so-called on-line machines. The KW-7 was connected between a teleprinter and a radio and automatically encrypted outgoing and decrypted incoming messages. The KW-7 device was intended for ship-to-land and ship-to-ship communication, communication took place in real time, and operators had to be present on both the transmitting and receiving sides (A History, Crypto Machines). During the attack on Pueblo, the ship was in constant contact with Kami Seya in Japan (Newton 1992). Kami Seya (near Yokohama) was at the time electronic reconnaissance center of the US Navy, it had several eavesdropping stations under it in Japan and one in South Korea (Naval Security). Messages between Pueblo and Kami Seye were enciphered (and deciphered) by the KW-7 machine.

The KW-37 was a US Navy system for sending messages to ships at sea, by encrypted radio-teleprinter messages. It was an improved version of the original German idea from the WW2 (Cipher Machines). On ships, the KWR-37 (“R” meant “Receiver”) was used to automatically decrypt those messages. In each network of that system, the new key was in use exactly at 0000 UTC and was valid until 2355 UTC that day. Without proper key, not only that messages could not be deciphered, but even number and length of those messages could not be known, because the transmitter on land continuously sent a signal (pseudo-random sequence) with which the actual message was "mixed". The teleprinter connected to the KWR-37 worked automatically and printed deciphered messages only when a valid key was set in the KWR-37 (Cipher Machines, Crypto Machines).

The KG-14 was a cryptological machine that could be used independently as a transmitter or receiver. Used in conjunction with KW-37 machine, it enabled simultaneous operation on multiple channels (frequencies). On ships, the KG-14 machines were set to work as receivers, connected to the KWR-37 devices (Crypto Machines). Keys for the KG-14 were taken away from Pueblo before she went on the mission, as well as the operating instructions. However, the machines themselves and the spare parts were retained, although without the keys the device could not be used (Cryptographic damage).

TSEC / KL-7 was an off-line encryption device. Off-line means that the message was first encrypted on the machine and handed over to the operator who would send it on, by radio-telegraphy or teleprinter. The KL-47 machine was made primarily for the US Navy, it was a more complex version of the KL-7 machine. The both versions were compatible. The KL-47 had punctuation marks on the keyboard in addition to letters and numbers, which the KL-7 did not have. When a message was enciphered by the KL-47 that was known to be deciphered by the KL-7, punctuation marks were replaced by certain abbreviations.

Basically, the KL-7 was an improved version of the German Enigma, which was also an off-line device and whose operation was based on rotors through which current passed. KL-7 also had rotors, 8 rotors were placed in the device at once (out of 12 available), according to the previously determined schedule and like with the Enigma an indicator was placed at the beginning of the message, so that on the receiving side the message could be deciphered.

The Americans made the KL-7 so that they successfully avoided all weak points of the Enigma. First, the KL-7 rotors were more complex than the Enigma rotors, their internal wiring changed from time to time, and the KL-7 rotors rotated around their axes during the enciphering / deciphering process (except for one that was stationary) on a more complex way than it was with the Enigma. In addition, unlike the Enigma, the KL-7 did not have a reflector, so a single letter (sign) could be enciphered by itself. This made the KL-7 a bit more complex than the Enigma, as there was an enciphering / deciphering switch on the machine, but the possibility of trying to deciphering the message without the key by using an assumed word (crib) in the encrypted message was avoided (A History, Crypto Machines, Cipher Machines, Crypto Museum).

The North Koreans found personal files of the crew members of Pueblo onboard the ship, in which they found information on their specialties, previous appointments, etc. Because of that the North Korean interrogators were at an advantage from the start. The personal files contained information of the entire career of an individual, among other things, the machines for which that individual was authorized to operate and/or maintain. The interrogators therefore immediately began to ask the right questions, and the prisoners could not give incorrect answers when North Koreans found documentation on Pueblo for most of these devices. Even without questioning the prisoners, the North Koreans would have come to know about the operation of those machines, but in this way they have saved themselves between 3 and 6 months. In addition, some machines that were not on Pueblo were listed in the personal files, so the prisoners had to answer questions about those machines too (Cryptographic damage).

During the interrogation, the interrogators used intimidation, convincing the prisoners that their country had left them, and mental and physical torture. Some examiners pretended to be "stupid," some showed their great knowledge. All those techniques are usual and sooner or later they achieve results, especially when interrogators have (or pretend to have) unlimited time and authority at their disposal and completely power on person they interrogate.

After exactly 11 months spent in captivity, the Pueblo crew crossed the "Bridge of No Return" at Panmunjom (Military Demarcation Line, border of the two Koreas) at 1130 hours on December 23, 1968, 82 survivors and one deceased- Fireman Duane D. Hodges.

Until that point, the NSA (National Security Agency) and the Navy did not know the exact extent of the damage caused by the capture of Pueblo. Because of that after their return to the US the Pueblo crew members were questioned about what exactly happened, how many equipment and documents were on Pueblo at the time of the capture (i.e. how many equipment and documents the crew destroyed before the capture) and what North Korean interrogators asked during the interrogation and what the crew members answered.

The conclusion was that the North Koreans (and “of course” the Soviets and Chinese) found out the cryptological principles of the machines they found on Pueblo, but that that alone did not mean they would be able to decrypt messages enciphered by those machines in the future. What the Americans did not know before the Pueblo crew returned to the US was that the North Koreans found old keys onboard Pueblo (for November and December 1967) which were presumed to have been destroyed no later than January 15, 1968.

The NSA did not consider the North Koreans recorded and stored U.S. enciphered messages (for possible later decryption) but believed the Soviets could do it (Cryptographic damage). In any case, with compromised traffic in the period 1-24 January 1968, there was a possibility of compromising traffic in the period November-December 1967.

The NSA concluded that by capturing Pueblo the other side gained insight into the way US ciphering machines work, but that that alone does not mean that in the future North Korea (and the Soviets) will be able to successfully decrypt messages ciphered by those machines. After all, American ciphering machines were designed to withstand the "attacks" of the other party, even if the other party knows their working principle.

However, the NSA also concluded that knowledge of the working principles of the machines would greatly facilitate the exploitation of the machines’ keys procured in an unauthorized manner. What worried the NSA in the long run was the possibility that "other countries" could improve their cryptographic security by learning about the principles of American machines, which would prevent the United States from successfully decrypting those countries' messages in the future (Report).

John Walker and the KGB- ciphers on sale

The capture of Pueblo was a surprise to the Soviets, and had North Korea asked them for their opinion before the action the Soviet Union would certainly have tried to prevent the action. Namely, despite the military and economic assistance they gave to their unpredictable and not always obedient friend, the aggravation of the situation on the Korean Peninsula was not interest of the Soviet Union. After the North Korean action, the Soviet Union publicly supported North Korea, what else the Soviets could, but at the same time they advised the North Koreans to calm down and resolve the incident politically, which eventually happened (Radchenko 2011).

After the capture of Pueblo the North Koreans, quite naturally, boasted to the Soviets of their "catch." According to some sources, a group of officers of the 6th Directorate (in charge of electronic reconnaissance) of the GRU (Soviet Military Intelligence Service) came to North Korea shortly after the capture and inspected Pueblo (Newton 1992). North Koreans provided the Soviets with at least some of the machines and documents found on Pueblo, including manuals for the operation and maintenance of the KW-7 and the machine itself (Heath 2005).

The Soviet officers naturally showed interest (it would be little strange if they did not) but it is for sure that some individuals in Moscow and the Soviet Embassy in Washington were very nervous after learning of the North Korean attack and the machines and documents found on Pueblo.

Usually, knowledge about the opposite side ciphers is more than welcome, but the Soviets have been receiving (i.e. buying) information on American naval ciphers from an American for some time, and when you have information on someone's ciphers, the least you want is that the other side begin to think about possibility that its ciphers have been compromised. The Soviets did not even need the machines captured on Pueblo, because they made them themselves with the help of the machines’ blueprints given to them by that American (Earley 1995).

Of course that the Soviets did not show their concern to the North Koreans. A few months after the capture of Pueblo, North Korean interrogators began asking the prisoners about the activities and results of the US Navy in reconnaissance of Soviet communications (Newton 1992). The questions asked by the North Koreans had to be very carefully put together in Moscow. On the one hand, the Soviets really wanted to know as much as possible about American electronic reconnaissance. On the other hand the Soviets knew that Pueblo crew would be released at some point and that after returning to the United States they would be questioned about the questions that the North Koreans were asking them and those questions had to convince the Americans of the security of their own ciphers.

The American who sold US Navy ciphers to the Soviets was John Walker. Many years later, he explained that he became a spy because he needed money, and other than US Navy secrets he could sell nothing (Heath 2005). And he did, for a full eighteen years, from 1967 to 1985. In fact, John Walker's life story was supposed to be an example of how (in this case) the Navy can turn a young delinquent into an honest person. And indeed, John Walker worked well in the Navy and in just ten years of service he was promoted to the rank of Warrant Officer and was a family man.

Outside, everything was perfect. Inside, John Walker was an alcoholic, as was his wife, and they had constant financial problems. Probably in that period John Walker at least sometimes remembered his father, a violent alcoholic who brought the family to bankruptcy and eventually left. Maybe in order to prove to himself that he is better than his father, he decided on something that eventually led to the same result - the destruction of the family. After he was transferred to work at a communications centre in Norfolk in November 1967, from which the Navy communicated with its submarines in the Atlantic, money was suddenly no longer a problem. All bills were paid and a luxury apartment was rented in Norfolk (Heath 2005).

It was possible because in October 1967 John Walker walked into the Soviet Embassy in Washington and offered his service. At the time (then) Colonel Boris Solomatin, an extremely capable operative, was a resident (head of the KGB station) at the Soviet embassy in Washington. As a rule, the resident never talks to the agents in person, but when his officers showed him the documents brought by the American, among other things there were the keys for the KL-47 machine (for next month) Solomatin realized the importance of the man who offered his service. Knowing that nobody play games with the ciphers Solomatin was almost certain that it was not an American provocation and decided to talk to that American in person. They talked in private, the conversation lasted two hours (Earley 1995, Prados 2014). Walker was open during the conversation, he was willing to submit documents in exchange for money and Solomatin liked that openness. Such agents, who work for money, are most liked by the intelligence services, because things are clear from the beginning, without additional complications that can occur with agents who work for other (for example ideological) reasons.

Solomatin knew that there was always the possibility of provocation, but he also knew that an agent-provocateur could be discovered if one knew what was really secret in one country and what was not, and that this could often be revealed by asking a simple question: whether the information offered to me will harm the country of the person giving me that information (Earley 1995). Solomatin did not know of any case where an intelligence service sent an agent-provocateur with information about ciphers, because as he himself explained, even when one service "feeds" another service with "garbage", a smart person can learn a lot from that garbage, information on the other side's way of thinking can be obtained. Ciphers are too serious for anyone to play with (Earley 1995).

Of course, there was a certain risk, that John Walker was actually an agent-provocateur. However, Solomatin liked risks, at least those that seemed justified to him. In a post-retirement interview, he said that without risk, there is no truly successful intelligence work (Earley 1995).

Soviet embassies from time to time received offers from individuals who offered their services. Sometimes they were provocateurs and sometimes fraudsters who wanted to make small money in exchange for worthless or false information. Those who really wanted to provide information (for money or because of ideology) were divided into two types, those who had potential and those who had not. The Soviets accepted further contacts only with those individuals whom they assumed to sincerely offered cooperation and had good potential — that is, good access to their country's classified information. It all depended on the assessment of the local resident, and the Soviets had problems immediately after WW2 because their residents at embassies too often rejected offers from people who wanted to provide information, for fear of agent-provocateurs (Serov 1964). Of course, those days (Stalin was still alive) mistakes were not punished by a career stalemate but by going to the Gulag (at best) so the hesitation of the residents could be understood.

To explain where that extra money came from, John Walker told the family he had found an extra job, but his wife did not believe the story. After she found instructions in their apartment that Walker had received from the KGB, how to deliver the materials, Walker admitted to his wife that he was spying for the Soviet Union, for $ 4,000 a month plus additional rewards. By comparison, his monthly salary in the Navy at the time was $ 725 (Heath 2005).

Despite making good money, John Walker felt a constant fear of being caught, so in mid-1969 he requested a transfer to San Diego, California, where he was an instructor at a school for radio operators. While working as an instructor at the school he carefully observed the students, intending to find a person suitable for recruitment, who would one day be his sub-agent.

In the meantime, the Soviets halved Walker's "salary" because he no longer had access to top-quality material. He needed the money so he therefore volunteered for duty at sea, and in late 1971 boarded supply ship USS Niagara Falls which was soon to set sail for a mission off the coast of Vietnam. The transfer was, for Walker and his Soviet bosses, a complete success. Walker was assigned to guard the classified material on board, and therefore had access to all classified documents, cipher keys etc. In addition, Walker regularly reported to be a courier when delivering classified material to other ships and bases on land. Namely, the USS Niagara Falls also served to deliver new cipher keys and other classified material to other ships, including aircraft carriers and submarines. In addition, Walker often offered to others to keep their classified material in his vault, for example the keys of the US Army ciphers in Vietnam (Heath 2005).

John Walker was onboard USS Niagara Falls for three years, from 1971 to 1974. During that time he did not literally (physically) steal the cipher keys, but copied them - first by a photocopier in the vault where the material was stored, and later by a camera. Because of the amount of work the camera given to him by the Soviets had worn out, so John Walker had to buy the new one (Heath 2005).

There was a war in Vietnam at the time, and the North Vietnamese would benefit from information the Soviets learned from decrypted American messages. However, although the Soviet Union sometimes gave some intelligence to its allies (Warsaw Pact members and other socialist countries), the information they received through John Walker the Soviets did not give to anyone. Giving this information to North Vietnam could threaten John Walker and the Soviets could not allow it (Earley 1995).

The Soviets paid Walker generously but after returning from Vietnam, Walker discovered that his family had discovered where he was hiding the money (a tin can buried in one corner of the garage) and that all the money had been spent. In addition, his wife indirectly told her surroundings that he was a spy. Probably no one believed her because she was intoxicated, but Walker decided to file for divorce, offering his wife $ 1,000 a month just to keep quiet plus monthly alimony ordered by the court to support the children.

Walker decided to leave the Navy as soon as he qualified for retirement. Between 1974 and 1976 he spent supervising the distribution of classified material in Norfolk and on July 31, 1976 he retired. After retiring, Walker remained in Norfolk, officially working as a private detective (Heath 2005). As a private detective Walker had coverage of why he was anywhere, at any time of the day or night, on any road, bar, hotel or parking lot, so the idea was really great.

Before retiring Walker recruited (in 1974) Senior Chief Jerry Whitworth, to whom he had once been an instructor in San Diego and had already selected him for possible recruitment. Between 1975 and 1982, Whitworth provided Walker with cipher keys and information on cipher machines, which Walker then provided to the Soviets. Walker later persuaded his brother Arthur Walker, a retired Lieutenant Commander who after retirement worked for a company that worked for the Navy. In 1981 and 1982, Arthur provided John Walker with certain classified information regarding the construction of ships (Espionage cases).

John's son Michael Walker was a yeoman in the Navy. In 1983, he was working at a naval air base in Virginia when he agreed to provide his father with classified information. In January 1984, Michael Walker was transferred to aircraft carrier USS Nimitz where he continued to collect information (McKinley 1987). Michael Walker copied more than 1,500 documents for his father, including documents on weapons systems, nuclear weapons control, command procedures etc. (Prados 2014). According to Boris Solomatin, John Walker and later Jerry Whitworth were by far the most useful to the Soviets in this whole story, for they delivered what nothing else can compare to — ciphers. Arthur Walker was the least useful to the Soviets (Earley 1995). Interestingly, Jerry Whitworth was at one time aboard USS Niagara Falls on the same duty as John Walker was (Prados 2014).

The following example shows the importance and mode of operation of John Walker and Jerry Whitworth. On June 30, 1979 John Walker had a meeting in Vienna with his Soviet connection. At the meeting Walker was told that the Soviets could no longer decrypt messages ciphered by the KW-37 cipher machine (although Walker regularly provided them with the keys) and that they thought some internal technical change had been made to the machine in the meantime. They have no problems with other machines, but they urgently need the technical information of the KWR-37. Jerry Whitworth obtained the requested information and submitted it to the Soviets through John Walker in November 1980 (Heath 2005).

In 1979, John Walker tried to recruit his daughter Laura who worked in the US Army Signal Corps. She later stated that John Walker used intimidation and emotional manipulation to recruit her and her brother Michael. He first told them that none of them would ever become successful, and then he told he would help them make a lot of money. Laura rejected the proposal and left the Army (Rasky 1985). John Walker also tried, in a roundabout way, to recruit his half-brother Gary, who was also in the Navy, but the latter refused (McKinley 1987).

Perhaps John Walker and the others would never have been discovered if Barbara Walker had not, at the urging of Laura Walker in November 1984, reported her ex-husband to the FBI. Barbara was outraged when she learned that John Walker had tried to recruit their daughter Laura. Although Laura declined the offer, she had problems because her ex-husband blackmailed her for it, seeking custody on their son (Heath 2005, Prados 2014). Probably the fact that John stopped paying Barbara money for silence also led to this development.

On February 25, 1985, the case was assigned to FBI Special Agent Robert Hunter. Evidence began to gather, the FBI tapped John Walker's phone conversations. At the behest of the FBI, Laura Walker telephoned her father, who showed interest in her return to the military, or perhaps the CIA… (Prados 2014).

On May 20, 1985, the FBI arrested John Walker, then Arthur Walker and Jerry Whitworth. NIS (Naval Investigative Service, predecessor of NCIS) arrested Michael Walker onboard USS Nimitz during the ship’s stay in Haifa, Israel (Prados 2014). Until the arrest of Michael Walker, Barbara and Laura Walker did not know that he was also involved in espionage and this knowledge hit them hard (Rasky 1985). Barbara Walker later said she would not have reported her ex-husband if she had known that her son was also involved in espionage (Soviet Spy).

Opportunity makes a thief

The question is- how it was possible that such person as John Walker was had access to Top Secret information. In fact, as a person sentenced to probation John Walker was not allowed to be admitted to the armed forces at all. However, John's brother Arthur persuaded the judge to lift the sentence and after that the recruiter did not ask too much - he was paid according to the number of people he managed to persuade to join the Navy. So, John Walker got a job and left a city where he would probably never get decent job, if he could get any job at all, and the judge got rid of a local delinquent. Everybody happy.

Members of the armed forces must have a security check of a certain degree, this of course also applied to John Walker. Regarding security checks, it should be borne in mind that the responsible services receive requests for checks of a large number of people, and they themselves have very limited capacity in time and people) so that checks are carried out according to strictly defined rules, in order to checked by as many people as possible. The questionnaire consists of specific questions to which there are only two answers - passed or failed. Not only does this save time but it reduces the subjective opinion of the officer performing the check. The downside of this practice is that it is possible to pass “under the radar”. In the beginning John Walker was a radioman for which he needed Secret clearance. For that level, the verification was done by checking the FBI and Department of Defense databases, which stored information at the federal level only and not at the state level or below. Since John Walker committed crimes at the level of his federal state in his youth, nothing was found in the databases of the FBI and the Department of Defense, and he of course did not state anything in the questionnaire he filled out.

As for the Top Secret clearance, the check procedure was of course much stricter, including checking for all possible crimes and misdemeanors and examining the work environment and neighborhood. In addition, as a person working with crypto-protective material, John Walker had to pass an even stricter check (TS-Crypto clearance). For that degree of verification, John Walker was proposed in 1962. The investigator studied the details of Walker's crime and conviction from his youth, but officially it was only one incident, although there may have been more than a dozen before that. In addition, at least from the outside, John Walker became an example of a man who was given a chance by the military and he used it in the best way. John Walker had been in the Navy for nine years, achieved excellent results at work (he was a radio operator on submarines) and progressed rapidly, by which time he was already a Chief Petty Officer and a family man.

As for examining the environment, the investigator asked colleagues at work and neighbors if John Walker could be gay, alcoholic, drug addict, if he has financial problems and if he has contacts with strangers. According to John Walker, everything went well and on December 29, 1964, he received the Top Secret / Crypto access clearance (Heath 2005). As for the questions, and the answers to them, the time when this happened should be taken into account. For example, homosexuality was then characterized as a mental illness and if John Walker had been homosexual and it had been revealed, he would have been fired immediately. On the other hand at that time alcohol consumption was normal, in fact more socially acceptable than complete abstinence.

The Very Secret clearance was valid for five years and was to be renewed in late 1969. However, the Defense Investigative Service (DIS) was so overwhelmed by the initial checks that they did not have time for subsequent ones, and all subsequent checks were postponed to several years. When it was John Walker's turn for a follow-up check, it was already 1972. Walker was aware of the situation and expected not to pass the new check. He spent money beyond his means, consumed alcohol and marijuana, openly maintained extramarital affairs, and in the end - his wife in an alcoholic state often complained to her friends and colleagues about his spying.

The way John Walker solved the problem of subsequent security checks would have looked incredible — if it hadn't really happened. At the time, he was aboard USS Niagara Falls and had access to the crew-members' personal files. Walker simply took his file, and file of another crew-member who had just passed a subsequent security check. In that other file he found a document confirming that a follow-up check had been made, a one-page form that had been stamped by the FBI. Walker copied that stamp on a copy paper, then (in uniform, to act officially) went to a local print shop where he had a duplicate stamp made. He then stole a blank form from the ship's warehouse, filled it out, stamped it, and put it in his personal file. He then returned both personal files to their places. All of this cost John Walker less than $ 3 (Heath 2005). Hard to believe but that really happened, John Walker "reinvestigated himself" and of course passed…

It was a big mistake of the DIS and it cannot be justified in any way. "Reinvestigations are more important than initial investigations. This is because almost all spies are recruited after they get access to classified material; very few initially apply for access intending to spy" (Heath 2005).

Because, opportunity makes a thief! And of course, no one should have access to his (or her) personal file!

John Walker's modus operandi

John Walker delivered information to the Soviets using dead drops, by the same way he received the money. In espionage dead drops are pre-determined places where one person leaves something (a message, money, etc.) that another person picks up after a while without the two people having to meet.

For the first two years, the Soviets requested that materials be delivered to them every two to three months, after which in 1970 they determined that materials be delivered once every six months (Heath 2005). John Walker delivered mostly old cipher keys to the Soviets, and the Soviets were completely satisfied with that. When John Walker retired (and recruited Jerry Whitworth) he offered the Soviets more frequent deliveries, but the Soviets refused. Of course, when it comes to a potentially long-term agent who also provides information of strategic importance, security takes precedence over speed.

At a meeting held in the summer of 1977 in Casablanca, Walker was reprimanded by his KGB contact for recruiting a new agent. John Walker agreed that meetings would then be held once a year in Vienna and that he would not recruit new agents (Prados 2014).

Probably the Soviets did not resent John Walker for recruiting a new agent, but for doing so without their approval, and through personal meetings in the future they wanted to avoid it. The Soviets sought to maintain contact with their agents by dead drops, as they considered it a safer way than personal meetings. However, in some cases personal meetings were necessary, and one of these cases was when the agent had his own agents (sub-agents), especially when he recruited them himself (Konovalov and Sokolov 1964). In addition, the Soviets used personal meetings with agents to study the agents, their potentials and talents, how honest the agents were, and how much they could be trusted (Bekrenev 1965).Personal meetings abroad were not used to deliver information, as John Walker continued to deliver information and receive money for it using dead drops in the United States.

The Soviets did not know much about John Walker's private life, probably only what he told them. They did not observe and follow Walker as this could attract unwanted attention (Earley 1995). It is to be expected that the local security service monitors a person who has access to classified information at least from time to time, and the presence of someone else who monitors that person would be discovered very soon.

The Soviets avoided maintaining personal meetings in the countries where their agents lived and worked. John Walker met only twice in person with the Soviets in the USA. The first of these meetings occurred when he walked into the Soviet Embassy in Washington and offered his service. The Soviet Embassy was under constant FBI surveillance, but the Soviets smuggled Walker (after accepting his offer for which he immediately received several thousand dollars) from the Embassy complex in a vehicle (Prados 2014). The FBI monitored the entrance to the Soviet Embassy, but was likely to be able to film en face only persons leaving the Embassy, for later identification. Of course that the Soviets knew that, so they acted in the stated way.

At most a month later, John Walker met with a Soviet naval intelligence officer (from the Soviet Embassy in Washington) in northern Virginia (northeast of Washington) outside a department store, during which John Walker handed over a large amount of documents and received instructions on dead drops system and money (Heath 2005, Prados 2014). After that, John Walker did not personally meet the Soviets for years, all communication was maintained exclusively through dead drops.

The dead drop system is not harmless either, because anyone can notice suspicious behavior of an individual by the roadside or in a forest, not to mention that embassy members are monitored (in any case, they must count on that possibility) and before arriving to the dead drop they must be sure that they are not under surveillance. In fact, the dead drop system is only slightly less dangerous than personal meeting with an agent, although of course it all depends on the country in which it all takes place.

Adolf Tolkachev was a Soviet engineer who provided Americans for years with extremely valuable information on avionics, cruise missiles, etc. Unlike John Walker, who used dead drops Tolkachev suggested using personal meetings instead of dead drops. Tolkachev explained that a face-to-face meeting is no more dangerous than using dead drops because in both cases, a CIA operative must make sure that he is not under surveillance before arriving to the place (of personal meeting or dead drop). In addition, a large amount of information can be delivered during a personal meeting, and most importantly for Tolkachev - this avoids the possibility that the information left in the dead drop does not accidentally fall into the wrong hands, and later analysis of the information reveal the source. The CIA accepted the proposal and after that Tolkachev and the CIA Moscow Station officers communicated almost exclusively through personal contacts (Royden 2003).

It all depends on what is usual in one country and what is not, the unusualness draws attention. This requires a good knowledge of the country in which one operates. Moscow and Norfolk were not the same then, and probably are not the same today.

After John Walker retired and informed the Soviets that he had in the meantime recruited Jerry Whitworth, the Soviets decided to hold personal meetings with John Walker, and those meetings were held exclusively abroad (not in the US).

The person (or persons) who met Walker probably did not belong to a local Soviet institution in that country (Soviet Embassy, Aeroflot, TASS, etc.) but it was someone who entered the country as a (for example) tourist or merchant, most likely not using a Soviet passport. Holding a personal meeting with an agent in a third country, with a representative of the Moscow Center (KGB Headquarters) who entered the country illegally (not as a citizen of the USSR) the Soviets considered almost completely safe (Bekrenev 1965, Konovalov and Sokolov 1964).

Conclusions

Examples of Americans caught spying for other countries showed that most of them had various professional and private problems, problems with alcohol, had problems with the law in their youth, problems with compliance with the rules, were lonely, they had narcissistic and psychopathic traits (Shaw and Sellers 2015).

It means that they were completely average people, because most people have problems with following the rules (but still follow them), civil servants who live on their salaries usually have financial problems, all at least sometimes have problems at work and in private life. Problem with alcohol is very relatively, it is not so much about the quantity but about how the individual behaves when consuming alcohol.

And the tendency to loneliness does not have to mean anything, because the most successful agents in history had an excellent ability to make friends, were extremely communicative, at first glance they would know what an individual likes or wants and they continued to play on that card.

Narcissism in itself does not mean that an individual will commit treason. Successful people are generally at least a little narcissistic - modesty and self-criticism do not help much in career. Yet, individuals who are narcissistic and do not achieve successful careers, at least not as much as they think they deserve, such people can indeed commit treason. As for psychopaths, they are the most dangerous, but they are very difficult to detect. The psychopaths successfully pass even the lie detector test, because they do not feel discomfort or fear, they actually do not care.

The first security check is more or less a formality and ensures that those who know they will never pass do not apply for a job at all. Some of those who passed security check are not perfect, but no matter how imperfect they may be, it would never occur to them to commit treason. In the end, it is always the individual who, impulsively or thoughtfully, decides to take that step, and even the best security check cannot predict that.

According to Boris Solomatin, John Walker was a talented man, he had a good sense of humor and was intelligent. He always wanted to be the center of attention and had unlimited ambition, he was shameless and cynical. The traits that helped him be such a successful spy were at the same time the main reason for his downfall. According to Solomatin, this is always the case with people like John Walker. After certain time they become reckless because they are convinced that they are smarter than others and invulnerable (Earley 1995).

All the listed character traits that Solomatin mentioned, and he should be trusted because he was a skilled and experienced operative, cannot be revealed by security check. The task of security screening is not to predict the future but to explore the past and present. Character traits of an individual can only be discovered through well-designed psychological testing.

The human factor has been and remains the weakest point of any data protection system. No measure, technical or organizational can ensure data protection if there is an insider who, for any reason is willing to give that data to someone outside. The following example shows the accuracy of this statement.

The rotors of the KL-7 were not allowed to open at the places where they were used, so as not to find out their internal wiring, but were sent to the NSA for repair or modification. This means that neither authorized machine operators nor authorized field service technicians were allowed to know the internal wiring of the rotor. However, the Soviets provided John Walker with a simple (but cleverly designed) small device, measuring approximately 7.5 x 10 cm, with which one could easily determine the internal wiring of the rotor without having to open the rotors.

John Walker was not the only one to whom the Soviets gave this device to detect the internal wiring of the KL-7 rotor. Warrant Officer Joseph Helmich was a member of the US Army who, while serving as a custodian of cryptographic material in France in 1963, offered the Soviet Embassy in Paris information about KL-7 for money. And after returning to the United States, he provided the Soviets with information about KL-7, until 1966. Helmich was arrested in 1981 and sentenced to life in prison. At Helmich, the FBI found the same device, which they later found at John Walker (Cipher Machines, Crypto Museum, Espionage cases).

The intelligence and counterintelligence services of any country rarely cooperate well with each other. As a rule, members of one service have a bad opinion of members of other service, and due to rivalry it is very difficult to share information with each other, and even when they have to share information they do it as little as possible. Besides, where competencies overlap, mostly no one does anything.

Therefore, it is good (if possible) to organize work of an agent or network in such a way that as many services as possible are in charge of the eventual discovery of that agent or network. In the end, several US services had to work together to get John Walker and his network caught with irrefutable evidence of their work. The FBI was in charge of counterintelligence work in the US, abroad it was supposed to be a joint action of the FBI and the CIA, and finally the NIS was in charge of counterintelligence in the Navy.

FBI Special Agent Robert Hunter, who led the John Walker case had a bad opinion of the NIS (Heath 2005). However, at the time Barbara Walker filed the complaint and later during the investigation Michael Walker was an active member of the Navy (the others were retired) so the NIS had to be involved (Prados 2014). Of course, the NIS agents probably had the same opinion about the FBI and the CIA.

The case of Edward Lee Howard is an example of how very difficult is to react properly after an individual has been spotted as a security threat. Howard and his wife were CIA employees and were prepared to work at the CIA Moscow station. Shortly before leaving for Moscow, Howard failed a polygraph test, it was a petty theft and drug use in his youth and in 1983 was forced to leave the CIA. Disappointed and financially troubled, Howard made contact with Soviet officials in Washington and arranged a meeting with KGB representatives in Vienna. Three meetings were held in Vienna in 1984 and 1985, at which Howard gave the Soviets, in exchange for money, information on the activities of the CIA Moscow station (Espionage Cases).

In August 1985, a Soviet defector to the west, Vitaly Yurchenko betrayed to the Americans two Soviet agents in the United States, Howard and a former NSA employee. Noticing that he was under surveillance, Howard became frightened and fled to the Soviet Union. Howard was well received by the Soviets, as well as some (much more) important defectors before him. Howard received an apartment in Moscow, a pension and a dacha (Russian type of cottage, an important status symbol) in the elite Zhukovka near Moscow. In that dacha Howard was found dead on July 12, 2002, allegedly Howard broke his neck in a fall down steps (Pincus 2002, Tavernise 2002).

Maybe it was really an accident. Or perhaps Howard still knew too much. Or someone just wanted that dacha. The dacha around Moscow has always been and will always be an important status symbol in Russia. Or, quite possibly, someone still wanted to portray Howard more important than he had ever been.

To this day, it is not known whether Jurchenko was an actual defector (who, however, soon after, in November 1985 penitently returned to Moscow, who forgave him everything…) or whether he was deliberately sent on a mission to the west. What is certain is that for the Soviets, exposing two relatively unimportant and in fact already spent agents at that time was a perfect fit. By distracting the Americans the Soviets managed to secure at least for a time their much more important agent, Aldrich Ames, who was still working at the CIA headquarters in Langley. Howard was not such an important agent, so it is possible that the privileges he received in the Soviet Union served to convince Americans that he was more important than he really was.

Allegedly, after Howard's case the CIA introduced changed the way it recruits its future employees and the way it treats those who (later) prove unsuitable for service abroad. The latter remain in service until their knowledge of current secrets diminishes (Pincus 2002). Reportedly, the CIA is tracking its former employees, presumably to see if any of them have suddenly started living a luxurious lifestyle after leaving the service.

As for the “current secrets”, defining them is not easy. During his preparations for work in Moscow, Howard was prepared to work with Adolf Tolkachev (Royden 2003). Not betrayed, Tolkachev could work for years more, which means that Howard would had to be kept in the service for years as well. Even longer than that, because the agent's actions remain secret even after the termination of that agent's active service, of course if the agent manages to remain undetected.

Even if the CIA had kept Howard in the service, he would have gotten a lower-ranking job in the US and would certainly have felt disappointment and anger and would probably have wanted revenge on the service for not trusting him enough. Finally, what kind of work in an intelligence or counterintelligence service could be given to persons who are shown to pose a potential security risk?

John Walker helped the Soviets to read the most secret messages of the US Navy for years. From these messages, the Soviets knew everything, what and how Americans do something, the way the Americans think, and most importantly — what Americans know (or think they know) and how they came to it.

The Soviets did not ask John Walker to provide them with the keys of the codes that were yet to be used, the old keys were enough to them. Here the Soviets acted very smart. The old keys are less well kept, so the danger to Walker was somewhat less, and the Soviets avoided the danger of acting in real time, or even preventively on some American move or action, after which Americans would probably doubt the security of their communications.

Probably it was decided by someone in the KGB, perhaps even Boris Solomatin who as an experienced intelligence officer knew that the American counterintelligence services were not the only danger for his agent, but also those in the USSR who could bring John Walker in danger because of their ambition or greed. Even the best agent will sooner or later be discovered if those to whom he submits the information uses it recklessly, and Solomatin knew that very well. The US

Navy sometimes gives a second chance to people who have made mistakes in the past. However, quite rightly, the Navy expects loyalty and gratitude from them.

Mistakes are severely punished, especially betrayal. And in the case of John Walker and his associates, the penalties were harsh. John and Michael Walker pleaded guilty to espionage at trial, John Walker was sentenced to two life sentences plus another ten years in prison and Michael Walker was sentenced to 25 years in prison. In exchange for a lighter sentence for his son, John Walker agreed to testify at the trial of Jerry Whitworth and gave the authorities all the information about what he handed over to the Soviets.

Arthur Walker was sentenced to life in prison and fined $ 250,000. At the time of sentencing, it was revealed that polygraph testing showed that Arthur Walker was able to submit data while still in active service, which would make the sentence higher.

Jerry Whitworth was sentenced to 365 years in prison and fined $ 410,000 (Espionage cases). Arthur Walker died in prison on July 5, 2014. John Walker died shortly thereafter, on August 28, 2014, he could be released on parole in 2015. Interestingly, Jerry Whitworth, in a separate trial, was punished more severely than John Walker. John and Arthur Walker were sentenced to life in prison, under federal law at the time, which meant they could be released on parole after 30 years. The judge who sentenced Whitworth to 365 years in prison did so that he could never be released on parole - for which he would have to live 106 years. Now he is 81.

Michael Walker served 15 years in prison and was released on parole in 2000. He was 22 years old at the time of his arrest (Soviet Spy). This text began with the North Koreans and will end with them. On April 15, 1969 North Koreans shot down a US Navy EC-121 SIGINT aircraft (PR-21) approximately 80 nautical miles off the North Korean coast, all 31 crew members of the EC-121 were killed. Talking to the Soviet ambassador to North Korea on April 16, 1969, the day after EC-121 was shot down, North Korean Deputy Foreign Minister Heo Dam said the Americans had not learned a lesson after the capture of USS Pueblo.

On the same day, the North Korean Foreign Minister Pak Seong-Ceol told the ambassador (among other things) as follows: “If we sit with folded arms when a violator intrudes into our spaces, two planes will appear tomorrow, then four, five, etc. This would lead to an increase of the danger of war. But if a firm rebuff is given, then this will diminish the danger of an outbreak of war. When the Americans understand there is a weak enemy before them, they will start a war right away. If, however, they see that there is a strong partner before them, this delays the beginning of war”(Mobley 2019).

The fact that the North Koreans explained their way of working to the Soviet ambassador shows that the North Koreans pursued their policy without asking anyone for permission to do anything, even such drastic measures as capturing a US Navy ship or shooting down a US Navy aircraft.

The Soviets really did not benefit from the capturing of USS Pueblo, quite the opposite. When one knows the principle of operation of an encryption machine and receives encryption keys regularly, it is not necessary to have the original machine at all.

During WW2 American code breakers managed to discover working principle of the Japanese Foreign Ministry's cipher machine (American code name for that Japanese cipher system was

Purple) and its keys, and based on that knowledge they made a device that simulated the operation of the original machine (Red and Purple). It was a great job of American code breakers who, unlike the Soviets in the Walker case, did not have an agent to provide them with machine information and keys.

If Americans could make replicas of the Japanese machine only on the basis of their knowledge of the principle of operation of the machine then the Soviets could make copies of American machines when Walker gave them blueprints of those machines right at the beginning, so they did not need to capture the original machines.

The North Koreans were expecting the arrival of the American SIGINT ship, only they were expecting another ship and not Pueblo. The North Koreans were warned by the Soviets and / or the Chinese about the presence of such a ship in the region. That ship was USS Banner (AGER-1) which had previously operated in the area, off the Soviet and Chinese coasts. In 1967, Banner spent a short time off North Korean coast (a day or two) but the North Koreans did not react (Newton 1992). A North Korean officer questioning Pueblo crew members stated that Banner was well known to him and that North Korea was waiting for an opportunity to capture her (Newton 1992). Perhaps the North Koreans were not acting when Banner was first in front of their coast because any action against Banner had to be approved from the very top, and that takes time. Approval may have arrived, but Banner has moved away from the area in the meantime. So the North Koreans waited for Banner to reappear. In fact, the North Koreans were a little confused at first, when they read the GER-2 designation on the Pueblo hull (Banner had the GER-1 designation), but they continued the action nonetheless (Newton 1992).

The place from which the attack on Pueblo was monitored and directed was at the radar station on Kukchi-bong. Kukchi-bong is a mountain located in the extreme south of North Korean east coast, near the demilitarized zone (the border of the two Koreas). It is probable that the NSA had a permanent eavesdropping station right on the other side of the border from which all available North Korean communications were constantly monitored, so the radio communications of the Kukchi-bong radar station with North Korean ships around Pueblo were also monitored.

The Kukchi-bong radar station told (between 1407 and 1408 hours) one of the torpedo boats that "the comrade who came down from the top is here" and that if it would be passed on to the submarine chaser commander, the commander would understand it (North Korean). Then Kukchi-bong said that he (the comrade from the top) thinks that they should go a little further and then board Pueblo because distance from the shore is still too great.

After noticing that the Pueblo crew was trying to destroy as many documents and equipment as possible (by fire and throwing into the sea), the submarine chaser ordered a quick action at 1430 hours (North Korean). From the mentioned conversation it can be seen that it was a prepared action, that someone "from the top" was present and that Pueblo was not in North Korean territorial waters at the time of the capture because the North Koreans even after they surrounded Pueblo waited to approach at least little closer to the shore and then board Pueblo.

The Soviets did not want to support North Korean plans, of which they knew nothing, and on February 26, 1968 Soviet leader Leonid Brezhnev spoke in Moscow with North Korean Deputy Prime Minister and Defense Minister Kim Ch’ang Bong. Brezhnev politely but decisively explained that the agreement on the alliance between the Soviet Union and North Korea has a purely defensive character and that no military solution on the Korean Peninsula suits the Soviet Union. It was reiterated that the Pueblo incident should be resolved politically without much delay. North Korean leader Kim Il Sung understood the message and in just a few days the situation calmed down (Radchenko 2011, pp. 61-68).

In late 2000 (then) US Secretary of State Madeleine Albright visited Pyongyang and during the visit the North Koreans moved Pueblo from Wonsan (east coast) to Pyongyang (west coast) through international waters. The North Koreans correctly concluded that the Americans would not act during the visit and so it happened, the USN was told “hands off” (USS Pueblo).

Sources:

A History of U.S. Communications Security (Volumes I and II), David G. Boak Lectures, National Security Agency (NSA), 1973 and 1981
http://www.governmentattic.org/18docs/Hist_US_COMSEC_Boak_NSA_1973u.pdf

Bekrenev, L. K. (1965) “Operational Contacts” Studies in Intelligence, Vol. 9 (Issue 1)
https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol9no1/html/v09i1a06p_0001.htm

Cipher Machines and Cryptology
https://www.ciphermachinesandcryptology.com

Crypto Machines
http://jproc.ca/crypto/index.html

Crypto Museum
https://www.cryptomuseum.com/crypto/usa/kl7/index.htm

Cryptographic damage assessment- USS Pueblo, AGER-2- 23 January- 23 December 1968, NSA, 28 february 1969 (DOCID: 3997687)
https://www.nsa.gov/news-features/declassified-documents/uss-pueblo/assets/files/damage-assessments/Section_V_Cryptographic_Damage_Assessment.pdf

Earley, Pete (1995) “Boris Solomatin Interview”
http://www.usspueblo.org/Aftermath/Pete%20Early-Boris%20Solomatin%20Interview.pdf

Espionage cases 1975-2004, Summaries and Sources, Defense Personnel Security Research Center Monterey, California, December 2004
URL http://cryptocomb.org/Espionage_Cases_75-04.pdf

Heath, Laura J. (2005) “An analysis of the systemic security weakness of the U.S. Navy Fleet broadcasting system, 1967-1974, as exploited by CWO John Walker” U.S. Army Command and General Staff College, Fort Leavenworth, Kansas
http://fas.org/irp/eprint/heath.pdf

Konovalov, A. A. and Sokolov, V. S. (1964) “Meeting with Agents” Studies in intelligence, Vol. 8 (Issue 2) https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol8no2/html/v08i2a05p_0001.htm

McKinley, Mike (1987) “Anatomy of treason- Tracking the Walker spy ring”, All Hands- Magazine of the U.S. Navy, No. 839, February 1987. https://media.defense.gov/2019/Apr/10/2002112657/-1/-1/1/AH198702.pdf

Mobley, Richard A. (2019) “Lessons from Four North Korean Shootdown Attempts during 1959-81”, Studies in Intelligence, Vol. 63, No. 2 https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-63-no-2/pdfs/Dangers-of-Airborne-Collection.pdf

Naval Security Group Station History http://www.navycthistory.com/NSGStationsHistory.txt

Newton, Robert E. (1992) “The Capture of the USS Pueblo and Its Effect on SIGINT Operations” U.S. Cryptologic History, Special Series, Crisis Collection, Vol. 7, Ft. George G. Meade: Center for Cryptologic History http://nsarchive.gwu.edu/NSAEBB/NSAEBB278/US_Cryptologic_History--The_Capture_of_the_USS_Pueblo.pdf

http://www.capecodtimes.com/article/20000217/news01/302179892

North Korean Navy voice reflections of U.S.S. Pueblo seizure, NSA, 7 February 1968 (DOCID: 3997511) https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/uss-pueblo/patrol-capture/North_Korean_Navy_Voice_Reflections_of_USSS_Pueblo_Seizure_Follow-Up_12.pdf

Pincus, Walter (2002) “CIA Defector Edward Lee Howard Said to Have Died in Moscow”, The Washington Post, 21 July 2002 http://www.udel.edu/globalagenda/2003/student/readings/CIAdefectordies.html

Prados, John (2014) “The John Walker Spy Ring and The U.S. Navy’s Biggest Betrayal”, USNI News, 2 September 2014 http://news.usni.org/2014/09/02/john-walker-spy-ring-u-s-navys-biggest-betrayal

Radchenko, Sergey S. (2011) “The Soviet Union and the North Korean Seizure of the USS Pueblo: Evidence from Russian Archives”, Woodrow Wilson International Center for Scholars, Cold War International History Project, Washington, 7 July 2011 https://www.wilsoncenter.org/sites/default/files/media/documents/publication/CWIHP_WP_47.pdf

Rasky, Susan F. (1985) “Daughter says John Walker pressed children to be spies”, The New York Times, 18 June 1985 http://www.nytimes.com/1985/06/18/us/daughter-says-john-walker-pressed-children-to-be-spies.html

Red and Purple
https://www.nsa.gov/about/cryptologic-heritage/center-cryptologic-history/pearl-harbor-review/red-purple/

Report on the Assessment of Cryptographic Damage Resulting from the Loss of the USS PUEBLO (AGER-2) (U), NSA, 28 July 1969 (DOCID: 4051684)
https://www.nsa.gov/news-features/declassified-documents/uss-pueblo/assets/files/lessons-learned/Doc_1.pdf

Royden, Barry G. (2003) "Tolkachev, A Worthy Successor to Penkovsky", Studies in Intelligence, Vol. 47, No. 3 URL https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol47no3/article02.html

Serov, Ivan A. (1964) "Work With Walk-ins", Studies in Intelligence, Vol. 8 (Issue 1)
https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol8no1/html/v08i1a02p_0001.htm

Shaw, Eric and Sellers, Laura (2015) "Application of the Critical-Path Method to Evaluate Insider Risks", Studies in Intelligence, Vol. 59, No. 2, June 2015.
https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-59-no-2/pdfs/Shaw-Critical%20Path-June-2015.pdf

"Soviet Spy Michael Walker Goes Free - No protest from CIA or Congress", Associated Press, February 17, 2000
https://www.jonathanpollard.org/2000/021700.htm

Tavernise, Sabrina (2002) "Edward Lee Howard, 50, Spy Who Escaped to Soviet Haven", The New York Times, 23 July 2002
http://www.nytimes.com/2002/07/23/world/edward-lee-howard-50-spy-who-escaped-to-soviet-haven.html

USS PUEBLO (AGER-2) - Official website of the USS PUEBLO (AGER-2) URL
http://www.usspueblo.org/index.html